System Guide

Microwave Data Systems Inc.

MDS *entra*NET

Access Point

Serial Remote

Ethernet Remote

Extended Range
IP Networking Transceivers

MDS 05-4055A01, Rev. A
OCTOBER 2003

industrial/wireless/performance

MDS

Contents

1 INTRODUCING THE entraNET SYSTEM 1

1.1 PRODUCT DESCRIPTION 3

1.1.1 Model Offerings 5

1.2 APPLICATIONS 5

1.2.1 Long Range Wireless LAN 5
Antenna Placement 6
Communication Rules 6
1.2.2 Multiple Protocols and/or Services 6
1.2.3 Upgrading an Older Wireless Network with Serial Interfaces 7
Replacing Legacy Wireless Products 7
Supplement legacy wireless network with IP services 8

1.3 SECURITY TECHNIQUES & TOOLS 8

1.3.1 Intrusion Detection via SNMP Traps 9

1.4 ACCESSORIES 9

2 TEST SETUP AND EVALUATION 11

2.1 INTRODUCTION 13

2.1.1 Connector Overview 13

2.2 STEP 1—CONNECT THE ANTENNA PORTS 15

2.3 STEP 2—MEASURE & CONNECT DC POWER 16

2.4 STEP 3—CONFIGURE THE TRANSCEIVERS 17

2.4.1 Access Point Configuration 17
Log In 17
AP Configuration Settings 18
2.4.2 Remote Unit Configuration 18
Log in 19
Set/Verify Network Address 19

2.5 STEP 4—CONNECT TERMINAL EQUIPMENT 20

2.5.1 Ethernet Remotes 20
2.5.2 Serial Remotes 20

2.6 STEP 5—CHECK FOR NORMAL OPERATION 20

2.6.1 Verifying Connectivity 21

Ethernet Remotes 21
Serial Remotes 22

3 AP MANAGEMENT 23

3.1 INTRODUCTION 25

3.1.1 Menu Structure 25
3.1.2 Differences in the User Interfaces 28
3.1.3 Accessing the Embedded Management System 29
3.1.4 Navigating the Menus 31
Web Browser 31
Telnet/Terminal Session 31
3.1.5 Logging Out of the entraNET Management System 32

3.2 BASIC DEVICE INFORMATION 32

3.2.1 Starting Information Screen 32
3.2.2 Main Menu 33

3.3 CONFIGURING NETWORK PARAMETERS 34

3.3.1 Network Configuration Menu 34
3.3.2 IP Configuration Menu 36
3.3.3 Wireless MAC Configuration 37
3.3.4 Mobility Configuration Menu 37
SNMP Configuration 38
3.3.5 Bridge Configuration Menu 39

3.4 CONFIGURING RADIO PARAMETERS 40

3.4.1 Radio Configuration Menu 40
Skip Zone Options Menu 41

3.5 CONFIGURING THE SERIAL INTERFACES 42

3.5.1 Overview 42
IP-to-Serial Services 42
Configuration 43
Serial Configuration Wizard 43
3.5.2 Serial Data Port Configuration Menu
(Local Serial-to-Remote Serial, or IP-to-Local Serial) 44
3.5.3 Remote Serial Gateway Configuration
(IP-to-Remote Serial) 47

3.6 SECURITY CONFIGURATION 49

3.6.1 Security Configuration Menu 49
3.6.2 Approved Remotes List Menu 50

3.7 WIRELESS NETWORK MENU 51

Remote Management Menu 52

Remote Database Menu 54
Endpoint Database Menu 55
Access Point Database Menu 56

3.8 STATISTICS/EVENT LOG 56

3.8.1 COM1 & 2 Serial Data Statistics Menus 58
3.8.2 Remote Serial Gateway Statistics Menu 58
3.8.3 Ethernet and Wireless Packet Statistics Menus 59
3.8.4 Radio Packet Statistics 61
3.8.5 Event Log Menu 61

3.9 DEVICE INFORMATION MENU 64

Device Names Menu 65

3.10 MAINTENANCE/TOOLS 65

3.10.1 Reprogramming Menu 66
Upgrading the AP's Firmware 67
3.10.2 Configuration Scripts Menu 70
A Brief Description of Configuration Files 71
Using Configuration Scripts 71
Sample of an Exported Configuration File 71
Editing Configuration Files 76
3.10.3 Ping Utility Menu 77
3.10.4 Authorization Keys Menu 78

4 REMOTE RADIO MANAGEMENT 79

4.1 INTRODUCTION 81

4.1.1 Programming Methods 81
Terminal Interface Mode 81
Remote Management via the AP 81
PC-Based Configuration Software 81
4.1.2 User Commands 81
Entering Commands 81
Command Responses 82
4.1.3 Minimum Remote Configuration 82
4.1.4 Detailed Command Descriptions 83

4.2 UPGRADING REMOTE FIRMWARE 93

5 SAMPLE CONFIGURATIONS 95

5.1 INTRODUCTION 97

5.1.1 IP-to-Local Serial Application Example 97
5.1.2 IP-to-Remote Serial Application Example 98
5.1.3 Point-to-Point, Serial-to-Serial Application Example 99

5.1.4 Point-to-Multipoint Serial-to-Serial Application Example 100
5.1.5 Mixed Mode Application Example 101
Operation and Data Flow 101

6 INSTALLATION 103

6.1 INSTALLATION 105

6.1.1 General Requirements 105
6.1.2 Site Selection 106
6.1.3 Terrain and Signal Strength 106
6.1.4 Antenna & Feedline Selection 107
6.1.5 Conducting a Site Survey 109
6.1.6 A Word About Radio Interference 109
6.1.7 How Much Output Power Can be Used? 111

6.2 dBm-WATTS-VOLTS CONVERSION CHART 113

7 TROUBLESHOOTING & RADIO TESTS 115

7.1 TROUBLESHOOTING 117

7.1.1 Interpreting the Front Panel LEDs 117
7.1.2 Troubleshooting Using the Embedded Management System 118
Ethernet Packet Statistics Menu 120
Serial Port/Remote Serial Statistics Menu 121
Diagnostic Tools 121
7.1.3 Using Logged Operation Events 121
7.1.4 Antenna Direction Optimization 122
Introduction 122
Procedure 122

8 TECHNICAL REFERENCE 125

8.1 DATA INTERFACE CONNECTORS 127

8.1.1 Ethernet/LAN Port (AP, Ethernet Remote) 127
8.1.2 COM1 Port (AP, Remotes) 128
8.1.3 COM2 Port (AP, Serial Remotes) 128

8.2 TECHNICAL SPECIFICATIONS 129

9 DEFINITIONS OF TERMS 133

Copyright Notice

This publication is protected by U.S.A. copyright law. Copyright 2003, Microwave Data Systems, Inc. All rights reserved.

ISO 9001 Registration

Microwave Data Systems adheres to the internationally-accepted ISO 9001 quality system standard.

Related Materials on the Internet

Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other valuable information are available on the MDS Web site at www.microwavedata.com.

About Microwave Data Systems Inc.

Almost two decades ago, MDS began building radios for business-critical applications. Since then, we've installed more than 500,000 radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on MDS-based wireless networks to manage their most critical assets.

The majority of MDS radios deployed since 1985 are still installed and performing within our customers' wireless networks. That's because we design and manufacture our products in-house, according to ISO 9001 which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, MDS is the wireless leader in industrial automation—including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for MDS and our customers as we look forward to further demonstrating our abilities in new and emerging markets.

As your wireless needs change you can continue to expect more from MDS. We'll always put the performance of your network above all. Visit us at www.microwavedata.com for more information.

OPERATIONAL & SAFETY NOTICES

RF Exposure

Professional installation required. The radio equipment described in this guide emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. Do not allow people to come closer than 23 cm (9 inches) to the antenna when the transmitter is operating in indoor or outdoor environments. More information on RF exposure is on the Internet at www.fcc.gov/oet/info/documents/bulletins.

UL/CSA Notice

This product is available for use in Class 1, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the National Fire Protection Association (NFPA) publication *NFPA 70*, otherwise known as the National Electrical Code.

The transceiver has been recognized for use in these hazardous locations by two independent agencies —Underwriters Laboratories (UL) and the Canadian Standards Association (CSA). The UL certification for the transceiver is as a Recognized Component for use in these hazardous locations, in accordance with UL Standard 1604. The CSA Certification is in accordance with CSA STD C22.2 No. 213-M1987.

UL/CSA Conditions of Approval: The transceiver is not acceptable as a stand-alone unit for use in the hazardous locations described above. It must either be mounted within another piece of equipment which is certified for hazardous locations, or installed within guidelines, or conditions of approval, as set forth by the approving agencies. These conditions of approval are as follows:

The transceiver must be mounted within a separate enclosure which is suitable for the intended application.

The antenna feedline, DC power cable and interface cable must be routed through conduit in accordance with the National Electrical Code.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver's installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

A power connector with screw-type retaining screws as supplied by MDS must be used.

WARNING

EXPLOSION HAZARD!

Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

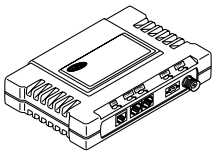
Refer to Articles 500 through 502 of the National Electrical Code (NFPA 70) for further information on hazardous locations and approved Division 2 wiring methods.

FCC Part 15 Notice

The transceiver complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device is specifically designed to be used under Section 15.247 of the FCC Rules and Regulations. Any unauthorized modification or changes to this device without the express approval of Microwave Data Systems may void the user's authority to operate this device. Furthermore, this device is intended to be used only when installed in accordance with the instructions outlined in this manual. Failure to comply with these instructions may also void the user's authority to operate this device.

Manual Revision and Accuracy

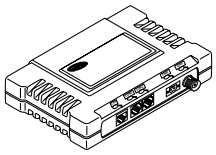
While every reasonable effort has been made to ensure the accuracy of this manual, product improvements may result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the MDS Web site at www.microwavedata.com.



1 INTRODUCING THE entraNET SYSTEM

Contents

1.1 PRODUCT DESCRIPTION 3
1.1.1 Model Offerings 5
1.2 APPLICATIONS 5
1.2.1 Long Range Wireless LAN 5
Antenna Placement 6
Communication Rules 6
1.2.2 Multiple Protocols and/or Services 6
1.2.3 Upgrading an Older Wireless Network with Serial Interfaces 7
Replacing Legacy Wireless Products 7
Supplement legacy wireless network with IP services 8
1.3 SECURITY TECHNIQUES & TOOLS 8
1.3.1 Intrusion Detection via SNMP Traps 9
1.4 ACCESSORIES 9



1.1 PRODUCT DESCRIPTION

This manual presents installation and operating instructions for the MDS entraNET 900 system. The manual is for use by those who will install, operate, and perform basic maintenance on the radio system.

The entraNET system is an easy-to-install wireless solution supporting long range Serial and Ethernet data transmission at speeds up to 106 kbps. The system includes an Access Point (AP) transceiver and two types of Remote transceivers—Serial or Ethernet. These units serve a variety of network configurations. Figure 1-1 shows each model in the entraNET family.

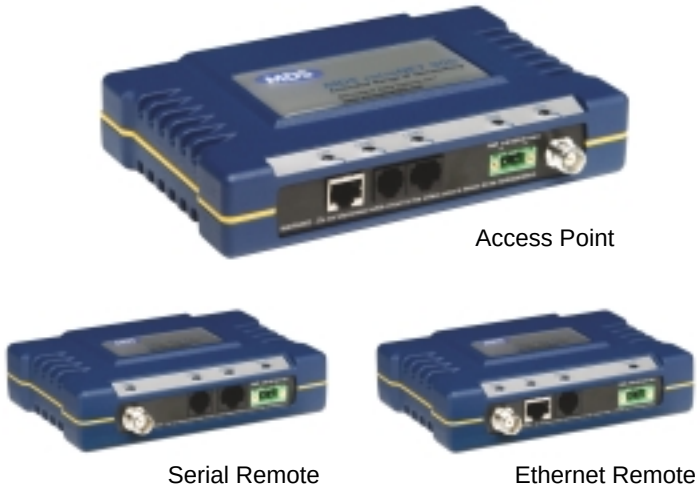


Figure 1-1. MDS entraNET 900 Transceivers

Media Access Control

MDS entraNET transceivers are equipped with a Media Access Controller (MAC) to ensure network access for stations with data to send. The MAC permits data to be sent from RTUs and other remote devices on an "on-demand" basis, preventing over-the-air data collisions and ensuring that the information gets through as intended. MAC functionality eliminates the need for active polling of Remotes, a key requirement in Report-by-Exception (RBE) applications.

Rugged Packaging

MDS entraNET units are housed in compact and rugged die-cast cases. They need only be protected from direct exposure to the weather. The transceivers are supplied with optional flat surface mounting brackets or 35 mm DIN rail brackets, depending on customer requirements.

Simple Installation

Basic installation typically employs an omni-directional antenna at the Access Point location and a directional antenna at each associated Remote site. The antenna is a vital link in the system and must be chosen and installed correctly. *INSTALLATION*, on Page 105 provides guidance on choosing proper sites and antennas.

To establish basic service, you simply connect an antenna, connect an Ethernet LAN to the AP, a serial or Ethernet device to the Remotes,

apply power, set a few operating parameters and you are done. No license is required for operation in the U.S.A., Canada, and many other countries. Check the regulations in your country before placing the units on the air.

Secure Operation

Network security is a vital issue in today's wireless world. The MDS entraNET system provides multiple tools to help you build a network that minimizes the risk of eavesdropping and unauthorized network access. Some are inherent in the radio's operation, such as the use of spread-spectrum transmission; other techniques include data encryption, enabling/disabling remote access channels, and password protection.

Remember, security is not a one-step process that can be simply turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. Section 1.3 on Page 8 contains additional information about entraNET's security features.

Robust Radio Operation

The transceivers are designed for frequency-hopping spread-spectrum operation in the license-free 900 MHz band. They can provide reliable communications at distances up to 30 miles (50 km) over line-of-sight signal paths. The units employ digital signal processing (DSP) techniques for high performance operation, even in the presence of weak signals or interference.

Multiple Services

Users with a mixture of equipment having Ethernet and serial data interfaces can employ a combination of both types of Remotes on the same cell or Access Point. This flexibility allows the transceiver to provide services in data networks that are on a migration path from legacy serial/EIA-232-based hardware to faster and more easily interfaced Ethernet systems.

Flexible Management

Configuration, troubleshooting and other maintenance activities may be performed locally or remotely. Four different modes of access are available: local RS-232 console, local or remote IP access through Telnet, and web browser access. SNMP functionality is planned for a future release. When available, this feature can be added to existing units by performing a simple firmware upgrade.

At AP transceivers, the text-based interfaces (RS-232 console and Telnet) are implemented in the form of easy-to-follow menus, and the terminal server configuration includes a "wizard" to help you set up the units correctly. At Remote units, a basic command line interface is used for this function.

Transceiver Features

The MDS entraNET 900's design makes installation and configuration an easy task, while allowing for changes in the future.

- Long Range—30 miles (50 km) over favorable, unobstructed terrain, with sufficient antenna height in a point-to-multipoint configuration

- Low Power Consumption—Sleep and Shutdown modes to enable solar-powered operation
- Single Radio Repeater *(Available soon—Contact MDS for information)*—Store & Forward capability to extend the range of a link or to work around obstructions without the expense and complexity of a traditional repeater.
- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to perform in high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of a network. Common attack events are logged and reported via alarms.
- Fast, 106 kbps data speed—Much faster than 9.6 kbps radios
- Simple Setup—Ethernet bridge configuration option requires minimal setup
- Serial Ports—Gateway for serial interface equipment to IP/Ethernet networks with embedded terminal server

1.1.1 Model Offerings

The MDS entraNET 900 system includes two primary radio types—Access Points and Remotes. In addition, two types of Remotes are offered—an Ethernet Remote, and a Serial Remote. Table 1-1 summaries the interface capabilities for each type.

Note: An Ethernet Remote will serve only one endpoint MAC address, even if a bridge or hub is used.

Table 1-1. MDS entraNET 900 Models and Data Interface Services

Model	LAN/ETH[1]	COM1[2]	COM2
Access Point	Yes	Yes	Yes
Ethernet Remote	Yes	Yes	No
Serial Remote	No	Yes	Yes

NOTES

1. “LAN” applies to AP connector, “ETH” applies to Remote connector.
2. Provides access to the embedded Management System.

1.2 APPLICATIONS

The following sections describe typical entraNET installations. Most installations will require planning or review by a network manager.

1.2.1 Long Range Wireless LAN

The wireless LAN is a common application of the entraNET 900 system. It consists of a central control station (Access Point) and one or

more associated Remote units, as shown in Figure 1-2 on Page 6. A LAN provides communications between a central WAN/LAN and Remote Ethernet endpoints. Ethernet Remotes can support only one Ethernet endpoint each.

The operation of the radio system is “transparent” to the computer equipment it is connected to. That is, the system behaves just as it would in a hardwired arrangement, with respect to data format and integrity.

Antenna Placement

The Access Point antenna is positioned at a location from which it can reliably communicate with all of the Remote units in the system. Commonly, this is a relatively high location on top of a building or communications tower. Over-the-air messages are exchanged at the Ethernet level. This includes all types of IP traffic.

Communication Rules

- A Remote transceiver can only talk over-the-air to an Access Point (AP), unless specially configured Direct Mode operation—*Available soon. Contact MDS for information*.
- Peer-to-peer communications between Remotes can take place indirectly through the AP.
- An AP can only talk over-the-air to Remote units, however two APs can communicate with each other through their Ethernet connectors utilizing a common LAN/WAN.

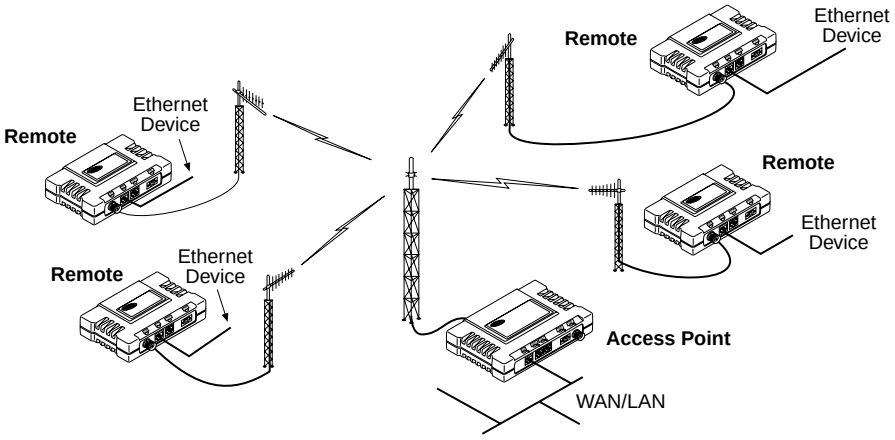


Figure 1-2. Typical wireless LAN

1.2.2 Multiple Protocols and/or Services

Prior to the introduction of the entraNET 900, two networks were often required to service two different types of devices (typically connected to different SCADA hosts). An entraNET 900 provides this functionality through a single AP radio. Each of the two (or more) groups of Remote radios can be connected via IP to different SCADA hosts, transporting different (or the same) protocols. Both data streams are completely inde-

pendent and the transceiver provides seamless simultaneous operation as shown in Figure 1-3.

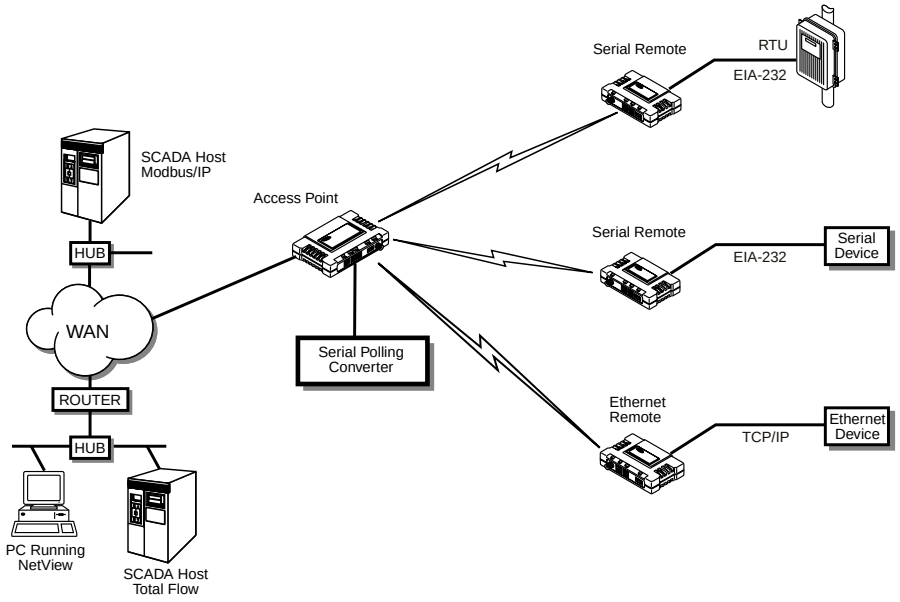


Figure 1-3. Multiple Protocol Network

By using a single AP the cost of infrastructure deployment is cut in half, with only one antenna, one feedline, and one lightning protector required. Other cost reductions come from the system as a whole, including reduced management requirements via the MDS NETview MS application. Finally, entraNET offers a nearly unlimited potential for future applications that run over IP and Ethernet.

1.2.3 Upgrading an Older Wireless Network with Serial Interfaces

Millions of wireless data products have been sold in the last two decades for licensed and license-free operation, many of them manufactured by Microwave Data Systems. There are several ways that these systems can benefit from employing MDS entraNET 900 equipment—key benefits include flexible serial and Ethernet interfaces, and higher data throughput.

MDS entraNET 900 units are well suited to replace leased or dial-up lines, or existing 900 MHz data transceivers by taking advantage of the transceiver's serial and Ethernet interfaces.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with MDS entraNET units with little or no special configuration. This equipment can be connected to entraNET units through the COM1 or COM2 port with a DB-25 to RJ-45 cable wired

for EIA-232 signaling. The COM2 port supports standard EIA-232 signaling and acts as a data-communications equipment device (DCE).

NOTE: Several previous MDS-brand products contained signal lines on their interface connectors that are not used or required on entraNET units. Consult the legacy equipment manual(s) for interface pinout information and connect only the required pins.

Supplement legacy wireless network with IP services

MDS entraNET 900 serial Remotes support most polled protocols. The serial interface (COM2) operates in two different modes: Connectionless serial-to-serial (UDP) and connection-oriented IP-to-serial (TCP).

In the UDP (connectionless IP-to-serial) mode, the transceiver supports point-to-multipoint IP-port to serial-port connectivity. In the TCP (connection-oriented IP-to-serial) mode, the transceiver supports point-to-point Ethernet/IP to serial port connectivity.

For more details on Serial Gateway interface modes see *"CONFIGURING THE SERIAL INTERFACES"* on Page 42.

1.3 SECURITY TECHNIQUES & TOOLS

Today the operation and management of an enterprise is becoming increasing dependent on electronic information flow. An accompanying concern becomes the security of the communication infrastructure and the security of the data itself.

The MDS entraNET 900 is capable of dealing with many common security issues. Table 1-2 profiles security risks and how the MDS entraNET 900 provides a solution for minimizing vulnerability.

Table 1-2. Security Risk Management

Security Risk	The MDS entraNET 900 Solution
Unauthorized access to the backbone network through a foreign remote radio	✓ Approved Remotes List Only those units included in the Approved Remotes list will connect
"Rogue" AP, where a foreign AP takes control of some or all Remote radios and thus remote devices	✓ Approved AP List A Remote will only associate to those APs included in its local authorized list of APs
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	✓ Failed-login lockdown After 3 tries, a transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.

Table 1-2. Security Risk Management

Security Risk	The MDS entraNET 900 Solution
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	✓ Remote login ✓ Local console login ✓ Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	✓ 900 MHz FHSS does not talk over the air with standard 802.11b cards ✓ The transceiver cannot be put in a “promiscuous” mode ✓ Proprietary data framing
Eavesdropping, intercepting messages	✓ 128-bit encryption
Key cracking	✓ Automatic Rotating Key algorithm
Replaying messages	✓ 128-bit encryption with rotating keys
Unprotected access to configuration via SNMP (available soon)	✓ Will enable/disable non-secure SNMP versions ✓ Will password-protect SNMPv3
Potential, ongoing attacks	✓ Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.)

1.3.1 Intrusion Detection via SNMP Traps *(Available soon)*

In addition to the operative tools and techniques, future releases of the MDS entraNET 900 will provide SNMP-based network management systems with traps (alarms) that report suspicious activities or events. These will include:

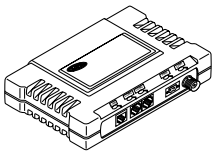
- Unauthorized AP serial number detected at Remote
- Unauthorized Remote serial number detected at AP
- Login attempt limit exceeded
  (Accessed via: Telnet, HTTP, or local)
- Successful login/logout
  (Accessed via: Telnet, HTTP, or local)

1.4 ACCESSORIES

MDS entraNET transceivers may be used with one or more of the accessories listed in Table 1-3. Contact the factory for ordering details.

Table 1-3. Accessories

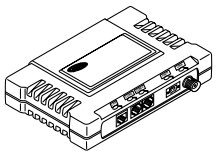
Accessory	Description	MDS Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc @ 2.5 A	01-3682A02
Omni-Directional Antennas	Rugged antennas well suited for use at Access Point installations. Consult with your factory Sales Representative for details	Contact factory
Yagi Antenna (Directional)	Rugged antennas well suited for use at Remote installations. Consult with your factory Sales Representative for details.	Contact factory
TNC Male-to-N Female Adapter	One-piece RF adaptor plug.	97-1677A161
TNC Male-to-N Female Adapter Cable	Short length of coaxial cable used to connect the radio's TNC antenna connector to a Type N commonly used on large diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly normally used to connect an Ethernet device or LAN to the transceiver. Both ends of the cable are wired identically. (Cable length ≈ 3 ft./1M)	97-1870A20
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to connect an AP to an Ethernet endpoint. (Cable length ≈ 3 ft./1M)	97-1870A21
RJ-12 to DB-9 Female Adapter	Allows access to Data Serial port COM1 on Remotes or APs.	73-2434A02
RJ-45 to DB-9 Female Adapter	Allows access to Data Serial port COM2 on Remotes or APs.	73-2434A12
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-9 male connector on one end, and a DB-9 female on the other end, 6 ft./1.8m long.	97-1971A03
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	29-1784A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2″ x 3″ plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Screws: 6-32/1/4″ with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
DIN Rail Mounting Bracket	Bracket used to attach the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4022A01 (Remote) 03-4022A02 (Access Point



2 TEST SETUP AND EVALUATION

Contents

2.1 INTRODUCTION 13
2.1.1 Connector Overview 13
2.2 STEP 1—CONNECT THE ANTENNA PORTS 15
2.3 STEP 2—MEASURE & CONNECT DC POWER 16
2.4 STEP 3—CONFIGURE THE TRANSCEIVERS 17
2.4.1 Access Point Configuration 17
Log In 17
AP Configuration Settings 18
2.4.2 Remote Unit Configuration 18
Log in 19
Set/Verify Network Address 19
2.5 STEP 4—CONNECT TERMINAL EQUIPMENT 20
2.5.1 Ethernet Remotes 20
2.5.2 Serial Remotes 20
2.6 STEP 5—CHECK FOR NORMAL OPERATION 20
2.6.1 Verifying Connectivity 21
Ethernet Remotes 21
Serial Remotes 22



2.1 INTRODUCTION

Prior to field installation, it is recommended that the radio system be set up in a controlled environment to become familiar with its operation. A tabletop network can be established to verify the basic operation of the system and allow tests of various network designs and configurations. Such a test can be performed with any number of radios.

This section describes the hardware setup and software configuration needed for a tabletop test. To simulate data traffic over the radio network, a PC or LAN will be connected to the Ethernet port of the Access Point and used to poll each Remote transceiver several times.

NOTE: For on-the-air testing, it is important to use a radio system Network Address and device IP addresses that are different from any currently in use in your region or network. This eliminates disruption to traffic on existing systems while you are testing the radios.

One technique for minimizing the chance of radio network address conflicts, is to use the last four digits of the radio's serial number.

2.1.1 Connector Overview

The illustrations below provide a reference to all of the interface connectors present on entraNET transceivers. A review of these items will assist you in making the connections described in the steps that follow.

Figure 2-1 shows the interface connectors for the Access Point transceiver.

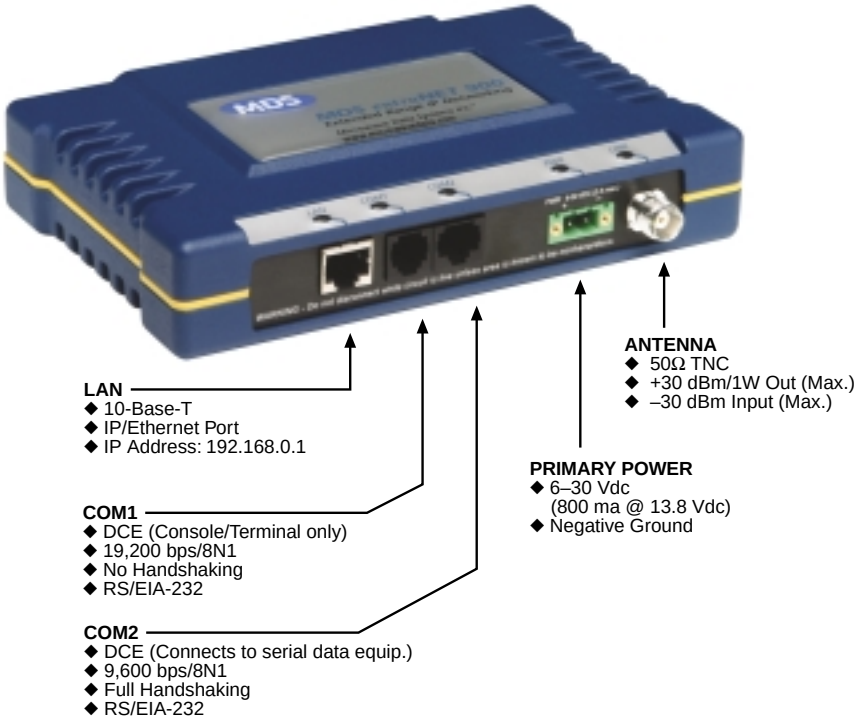


Figure 2-1. Access Point Interface Connectors

Figure 2-2 shows the interface connectors for the Ethernet Remote transceiver.

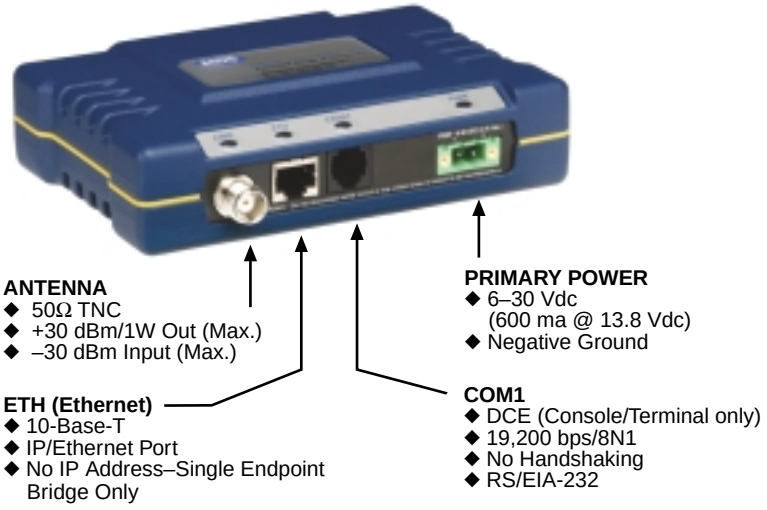


Figure 2-2. Ethernet Remote Interface Connectors

Figure 2-3 shows the interface connectors for the Serial Remote transceiver.

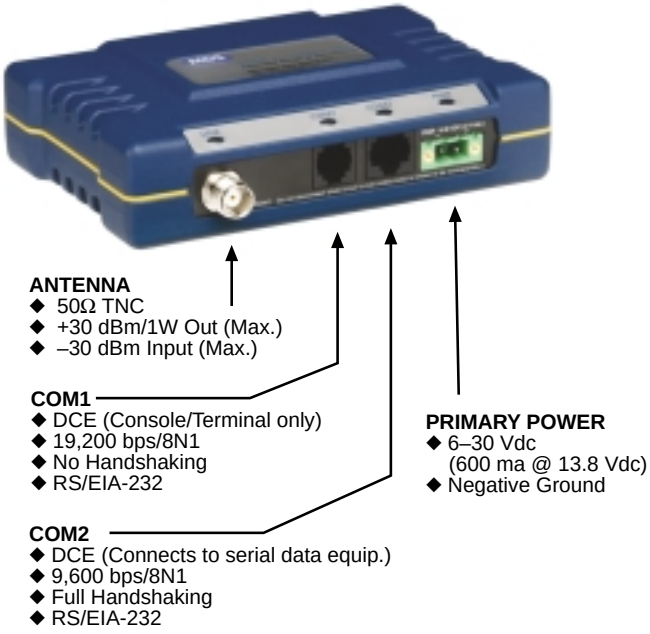


Figure 2-3. Serial Remote Interface Connectors

2.2 STEP 1—CONNECT THE ANTENNA PORTS

Figure 2-4 is a drawing of a tabletop arrangement. Connect the antenna ports of each transceiver as shown. This will provide stable radio communications between each unit while preventing interference to nearby electronic equipment.

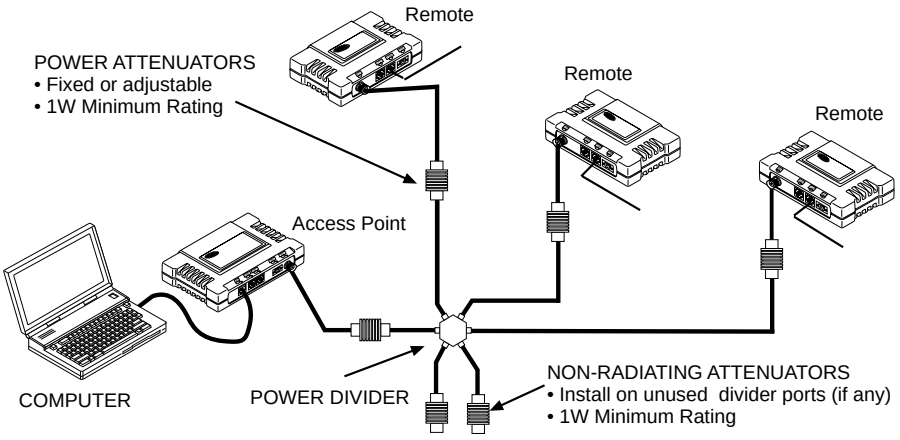


Figure 2-4. Typical Setup for Tabletop-Testing of Radios

NOTE: It is very important to use attenuation between all units in the test setup. The amount of attenuation required will depend on the number of units being tested and the desired signal strength (RSSI) at each transceiver during the test. In no case should a signal greater than –30 dBm be applied to any transceiver in the test setup. A transmit RF power output level of +20 dBm is recommended. (See *"Radio Configuration Menu"* on Page 40.)

2.3 STEP 2—MEASURE & CONNECT DC POWER

The power applied to transceivers must be within 6–30 Vdc and be capable of continuously providing a minimum of 11 Watts. (Typical power consumption is: 800 mA @ 13.8 Vdc (AP) and 600mA @13.8 Vdc (Remote). A power connector with screw-terminals is provided with each unit. Strip the wire leads to 6 mm (0.25"). Be sure to observe proper polarity as shown in Figure 2-5 with the positive lead (+) on the left.

NOTE: It will take about 30 seconds for the AP transceiver to power up and be ready for operation. The Remote requires approximately 5 seconds.

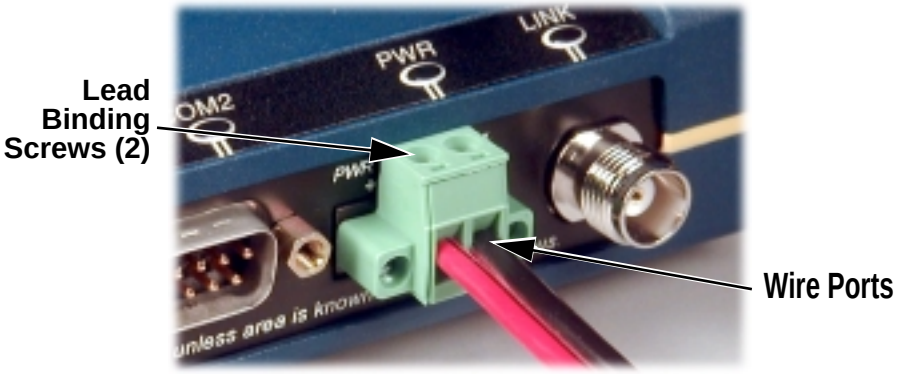


Figure 2-5. Power Connector (Polarity: Left +, Right –)

CAUTION
POSSIBLE EQUIPMENT DAMAGE

The transceiver must be used only with negative-ground systems. Make sure the polarity of the power source is correct. The unit is protected from reverse polarity by an internal diode and fuse.

2.4 STEP 3—CONFIGURE THE TRANSCEIVERS

2.4.1 Access Point Configuration

The Access Point must be configured first, as Remote transceivers depend on the AP's beacon signal to achieve a "connected" (linked) state. To configure the Access Point, connect a PC with the radio's COM1 port and establish a terminal session (i.e., HyperTerminal) using the following data parameters: 19200 bps, 8 bits, no parity, one stop bit (8N1), flow control disabled, VT100 emulation.

Alternatively, you can connect a PC's Ethernet port to the AP's LAN port using an Ethernet crossover cable. Note: This method requires that the radio have a valid IP address programmed—it will not contain an appropriate IP address as shipped from the factory.

Figure 2-6 shows the basic setup for configuring an AP with a personal computer.

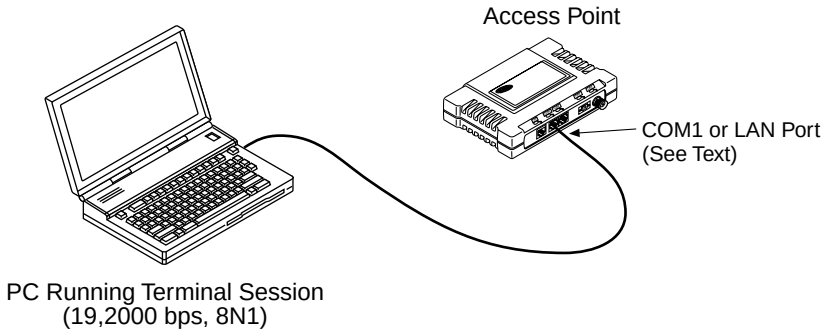


Figure 2-6. AP Configuration Setup

Log In

Log into the AP as follows:

1. Press the ENTER key to receive the **login** prompt. The COM1/LAN LED flashes to indicate data communications.

2. At the **login** prompt, enter the username (**admin** is the default username). Press ENTER.

3. At the **Password** prompt, enter the password. (**admin** is the default password). Press ENTER. The Starting Information Screen appears.

4. Review the current settings and make any necessary changes. Refer to *AP Configuration Settings*, on Page 18 for configuration guidance.

5. Repeat Steps 1–4 for any other AP units in your radio system.

NOTE: The Management System supports the use of "configuration scripts" to aid in uniformly configuring multiple transceivers. This time-saving technique is detailed in *Using Configuration Scripts*, on Page 71.

AP Configuration Settings

Table 2-1 provides a listing of key AP operating parameters, their default settings, and values or range. Typically, these are the only settings that need to be set or reviewed for a basic check of the radio system. A complete list of AP commands is provided on Page 23 in the section titled *AP Management*.

Table 2-1. Basic AP Configuration Defaults

Item	Mgt. System Location	Default	Values/Range
IP Address	**Main Menu> Network Configuration>IP Configuration**	192.168.1.1	Contact your Network Administrator
IP Network	**Main Menu> Network Configuration>IP Configuration**	255.255.0.0	
Radio Net Address*	**Main Menu> Network Configuration>Wireless Mac Configuration**	100	1-20000 (See note below)
TX Power	**Main Menu> Radio Configuration>**	+30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watts)
Password	**Main Menu> Security Configuration> User Passwords**	**admin** (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case

* It is recommended that the Network Address be set to the last four digits of the AP's serial number. This reduces the chance of conflict with other nearby entraNET systems.

2.4.2 Remote Unit Configuration

Once the Access Point is up and running, move the computer connection to each of the Remote units to configure them for operation with the AP. To configure the Remote radio, connect a PC to the unit's COM1 port and establish a terminal session (i.e., HyperTerminal) using the following data parameters: 19200 bps, 8 bits, no parity, one stop bit (8N1), flow control disabled, VT100 emulation.

Figure 2-6 shows the basic setup for configuring a Remote with a personal computer.

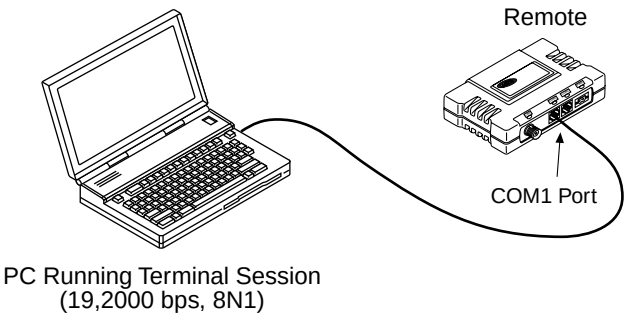


Figure 2-7. Remote Configuration Setup

Log in

Follow these steps to login to the radio.

1. Press a few ENTER keystrokes to receive the **entranet>** prompt. (The COM1/ETH LED blinks to indicate data communication.)

2. At the **entranet>** prompt, type **login**. Press ENTER.

3. At the next prompt, enter username (default username is **admin**). Press ENTER.

4. At next prompt, enter Password (default password is **admin**). Press ENTER. The unit is now ready to accept commands.

Set/Verify Network Address

The only setting normally required for initial checkout of a Remote radio is the Network Address. All radios in a given network *must* be programmed with the same network address as the AP or communication will not be possible. Follow the steps below to check the address, and program a new one if necessary.

1. Enter the **RADIO NETADDR** command. This displays the radio's currently programmed network address.

2. If changes are required, enter the **RADIO NETADDR= <netaddr>** command, where **<netaddr>** is a number from 1 to 20000. (The network address of the Remote radio *must* match that of the AP.)

3. Verify that the LINK LED lights to indicate successful connection with the AP. (It may take several seconds for the LED to light).

4. Repeat Steps 1–3 for each Remote radio to be installed in the network.

This concludes the basic setup of a Remote radio. A full listing of Remote programming commands is given in *CHAPTER-4 REMOTE RADIO MANAGEMENT* beginning on Page 79.

With all units connected, you are ready to connect data devices to the transceivers so that their operation can be tested over the wireless network.

2.5 STEP 4—CONNECT TERMINAL EQUIPMENT

This step describes connection of external data equipment to the Remote radio. Verify that your transceiver is capable of supporting your devices. (See *Table 1-1 . MDS entraNET 900 Models and Data Interface Services,* on Page 5 for a summary of model capabilities.)

Be sure not to overload the radio network with high bandwidth LAN traffic during this test. Refer to *Bridge Configuration Menu*, on Page 39 for more information.

2.5.1 Ethernet Remotes

NOTE: Verify that the Remote's ETH (Ethernet) port is enabled (on) using the **MODE** command. If it is not, use the **MODE=ON** command to enable the port.

Connect an Ethernet endpoint to the Remote's ETH port. The ETH port will support any Ethernet-compatible device. This includes a device that uses the Internet Protocol (IP).

2.5.2 Serial Remotes

Connect a serial device to the Remote's COM2 port and verify that the port settings are compatible with the connected device (baud rate, data format, etc.)

2.6 STEP 5—CHECK FOR NORMAL OPERATION

With the data equipment connected, you are ready to check the transceivers for normal operation.

Observe the transceiver LEDs on the top cover for the proper indications. In a normally operating system, the following LED indications will be seen within 30 seconds of start-up:

- PWR—Lit continuously
- LINK—Lit continuously

- LAN/ETH (Ethernet units)—On or blinks intermittently
- COM2—Blinks to indicate data communications

Table 2-2 provides details on the LED functions for Remotes and AP radios.

Table 2-2. Transceiver LED Functions

LED Label	Activity	Indication
LAN/ETH	ON	LAN or endpoint detected
	Blinking	Data TX/RX
	OFF	LAN not detected
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity
COM2	Blinking	Data TX/RX
	OFF	No data activity
PWR	ON	Primary power (DC) present
	Blinking	Unit in “Alarmed” state
	OFF	Primary power (DC) absent
LINK (Access Point)	ON	Lights when radio has finished its boot cycle. Remains lit.
LINK (Remote)	ON	Connected to AP
	OFF	Not connected to an AP

2.6.1 Verifying Connectivity

Ethernet Remotes

If the radio network is operating properly based on observation of the unit’s LEDs, you can use the **PING** command from the AP to verify the link integrity between the Access Point and an endpoint-device connected to the Remote radio. Figure 2-8 shows the a typical arrangement for this test.

NOTE: To conduct a Ping test, an Ethernet-enabled device must be connected to the Remote, and it must have a compatible IP address. Remote radios do not have an IP address and cannot be verified directly using this method.

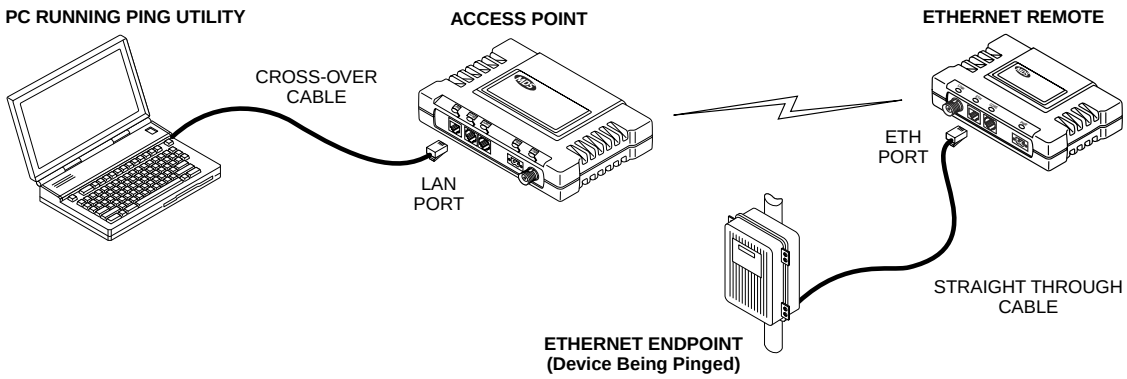
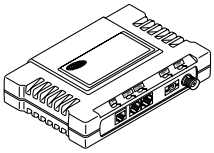


Figure 2-8. Ping Test Setup
(To test connectivity between an AP and an Ethernet Endpoint)

Serial Remotes

To check connectivity with Serial Remotes, refer to *Serial Data Port Configuration Menu (Local Serial-to-Remote Serial or IP-to-Local Serial)*, on Page 44. This section contains details on establishing an IP-to-serial or serial-to-serial connection.



3 AP MANAGEMENT

3.1 INTRODUCTION 25

3.1.1 Menu Structure 25
3.1.2 Differences in the User Interfaces 28
3.1.3 Accessing the Embedded Management System 29
3.1.4 Navigating the Menus 31
Web Browser 31
Telnet/Terminal Session 31
3.1.5 Logging Out of the entraNET Management System 32

3.2 BASIC DEVICE INFORMATION 32

3.2.1 Starting Information Screen 32
3.2.2 Main Menu 33

3.3 CONFIGURING NETWORK PARAMETERS 34

3.3.1 Network Configuration Menu 34
3.3.2 IP Configuration Menu 36
3.3.3 Wireless MAC Configuration 37
3.3.4 Mobility Configuration Menu 37
SNMP Configuration 38
3.3.5 Bridge Configuration Menu 39

3.4 CONFIGURING RADIO PARAMETERS 40

3.4.1 Radio Configuration Menu 40
Skip Zone Options Menu 41

3.5 CONFIGURING THE SERIAL INTERFACES 42

3.5.1 Overview 42
IP-to-Serial Services 42
Configuration 43
Serial Configuration Wizard 43
3.5.2 Serial Data Port Configuration Menu (Local Serial-to-Remote Serial, or IP-to-Local Serial) 44
3.5.3 Remote Serial Gateway Configuration (IP-to-Remote Serial) 47

3.6 SECURITY CONFIGURATION 49

3.6.1 Security Configuration Menu 49
3.6.2 Approved Remotes List Menu 50

3.7 WIRELESS NETWORK MENU 51

Remote Management Menu 52
Remote Database Menu 54
Endpoint Database Menu 55

Access Point Database Menu 56

3.8 STATISTICS/EVENT LOG 56

3.8.1 COM1 & 2 Serial Data Statistics Menus 58
3.8.2 Remote Serial Gateway Statistics Menu 58
3.8.3 Ethernet and Wireless Packet Statistics Menus 59
3.8.4 Radio Packet Statistics 61
3.8.5 Event Log Menu 61

3.9 DEVICE INFORMATION MENU 64

Device Names Menu 65

3.10 MAINTENANCE/TOOLS 65

3.10.1 Reprogramming Menu 66
Upgrading the AP's Firmware 67
3.10.2 Configuration Scripts Menu 70
A Brief Description of Configuration Files 71
Using Configuration Scripts 71
Sample of an Exported Configuration File 71
Editing Configuration Files 76
3.10.3 Ping Utility Menu 77
3.10.4 Authorization Keys Menu 78

3.1 INTRODUCTION

The MDS entraNET 900 AP is equipped with an embedded management system that is accessible through various data interfaces. These include the COM1 (serial) port and the LAN (Ethernet) port. Essentially the same capabilities are available through any of these paths. To access any of the interfaces, you must enter a valid password and username.

Future firmware releases for the transceiver will also support SNMP-based management tools such as Microwave Data Systems' *NETview MS*™. For support of other software, a set of MIB files will be available for download from the Microwave Data Systems' Web site at www.microwavedata.com. Contact MDS for information on the availability of these tools.

Coverage of the entraNET Management System and its functions are divided into nine functional groups in this chapter as follows:

- 3.3 *CONFIGURING NETWORK PARAMETERS*, (beginning on Page 34)
- 3.4 *CONFIGURING RADIO PARAMETERS*, (beginning on Page 40)
- 3.5 *CONFIGURING THE SERIAL INTERFACES*, (beginning on Page 42)
- 3.6 *SECURITY CONFIGURATION*, (beginning on Page 49)
- 3.7 *WIRELESS NETWORK MENU*, (beginning on Page 51)
- 3.8 *STATISTICS/EVENT LOG*, (beginning on Page 56)
- 3.9 *DEVICE INFORMATION MENU*, (beginning on Page 64)
- 3.10 *MAINTENANCE/TOOLS*, (beginning on Page 65)

Each of these sections has a focus that is reflected in its heading. The section you are now reading will provide you with information on connecting to the entraNET AP, how to navigate through its menus, and how to perform some top-level configuration tasks.

Remote commands are presented separately in Chapter *4 REMOTE RADIO MANAGEMENT*, (beginning on Page 79).

NOTE: Parameter options/ranges, and any default values are displayed at the end of the field description between square brackets. The default value, is always shown last in a series of items. For example: [range, options or description**; default**]

3.1.1 Menu Structure

The following illustrations (Figure 3-1 and Figure 3-2) show an overall view of the entraNET Management System (MS). Detailed information for screens and menu items is provided on the following pages.

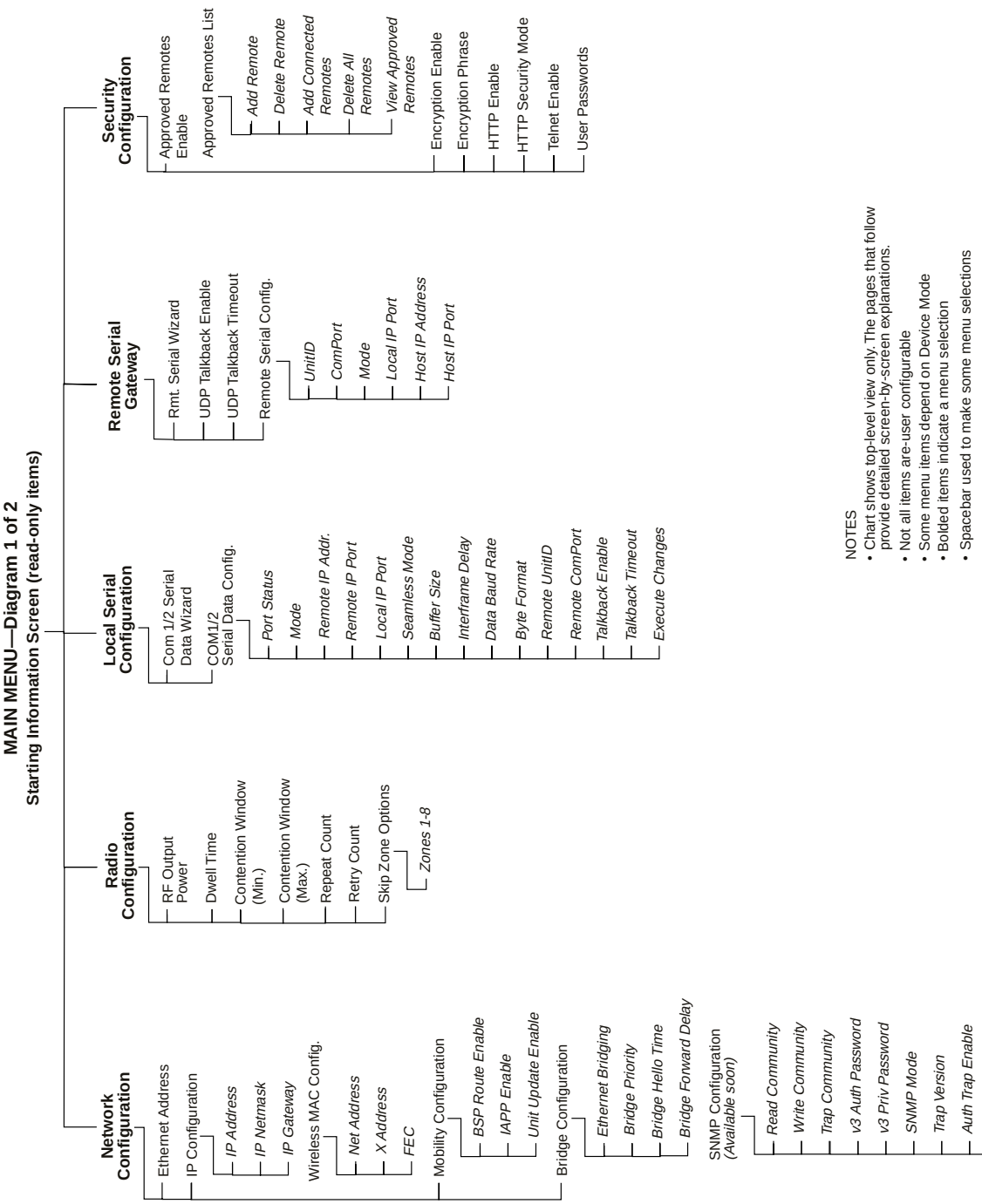


Figure 3-1. *entraNET* Management System Menu Flowchart (Chart 1 of 2)

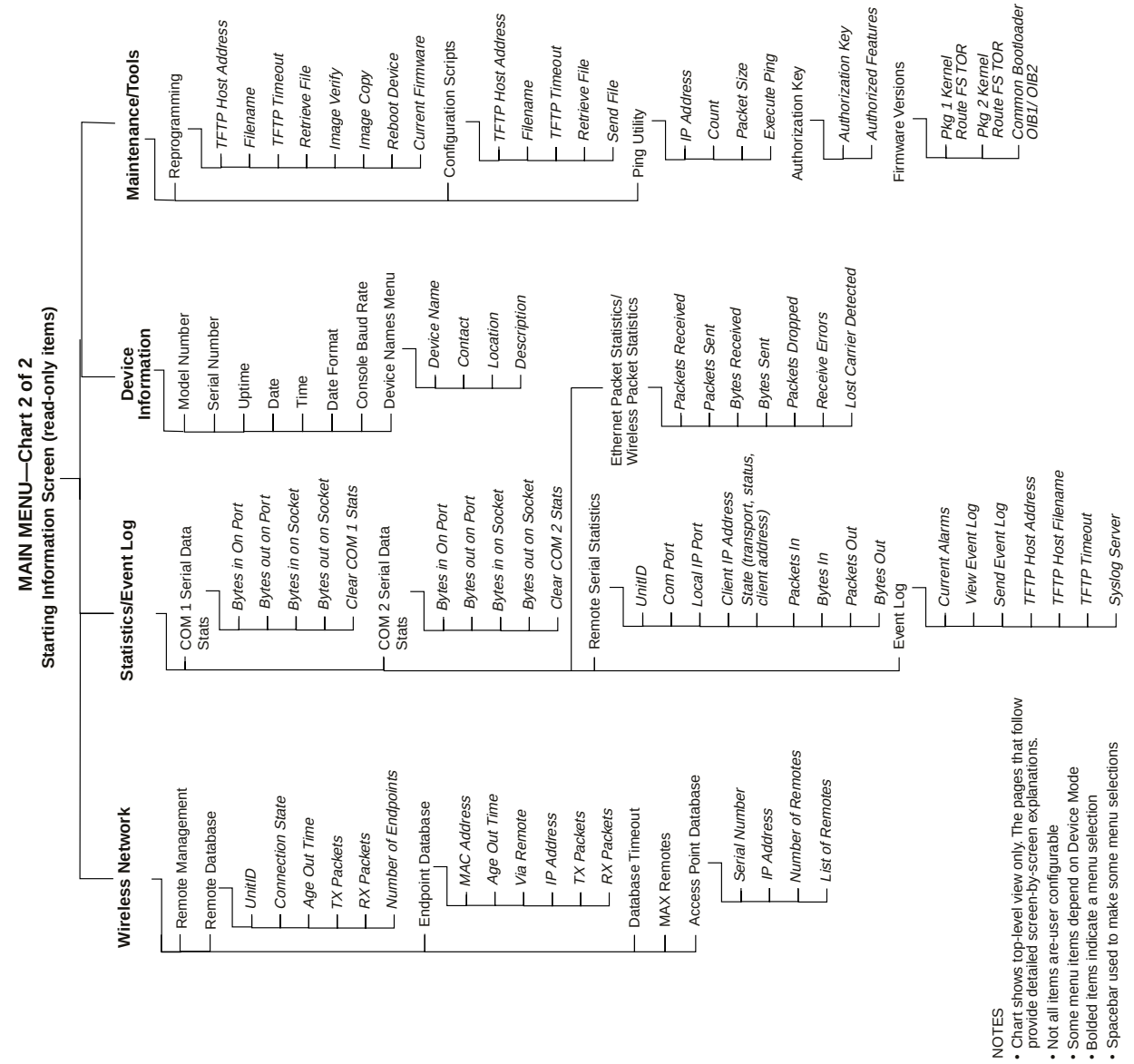


Figure 3-2. *entraNET* Management System Menu Flowchart (Chart 2 of 2)

3.1.2 Differences in the User Interfaces

There are slight differences in navigation between Telnet, Terminal and Web interfaces, but for the most part, the content of screens will be the same. There area few differences in capabilities, as the communications tool is driven by limitations of the access channel. Below are samples of the Starting Information Screen as seen through a terminal session and a web browser.

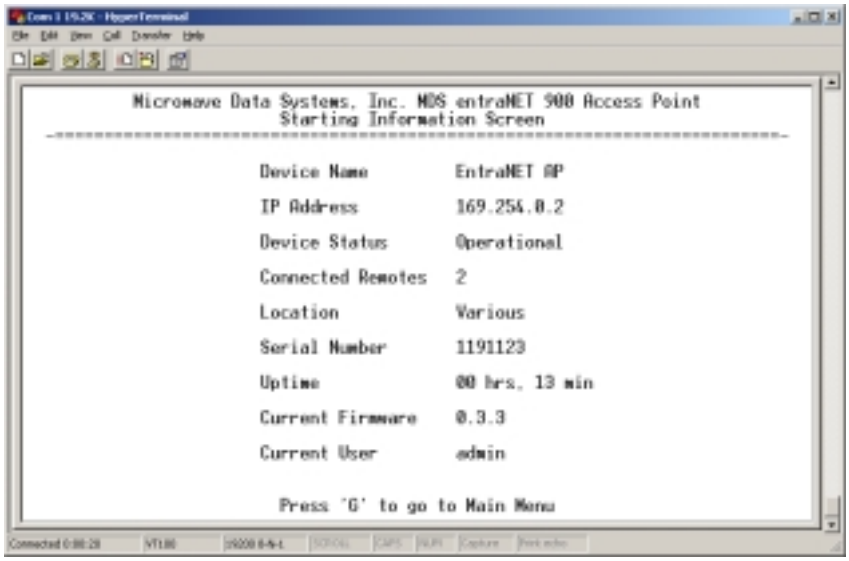


Figure 3-3. View of entraNET MS Using a Terminal Session (Telnet Similar)

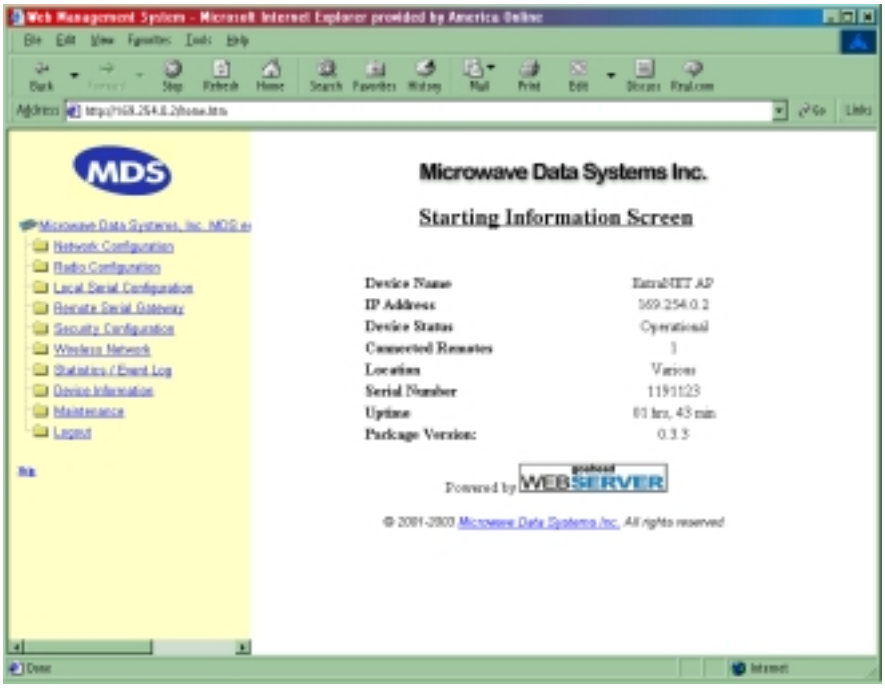


Figure 3-4. View of the entraNET MS with a Browser

3.1.3 Accessing the Embedded Management System

The menu-based management system provides access to view and configure many unit parameters and provides you with basic diagnostic and maintenance tools. There are several ways to gain access to the entraNET Management System.

- **Terminal-Emulator**—Use a terminal emulator program on your PC, such as HyperTerminal, connected directly to the MDS entraNET 900 COM1 port via a serial cable.
- **Telnet**—Text-based access to the Management System through the Ethernet interface (AP only).
- **Web Browser**—Connect to the entraNET units using a Web browser on a local PC connected directly to the transceiver's LAN port or associated network (AP only).

When you use Telnet or a Web browser to communicate with the transceiver, you will need to know the unit's IP address, the User Name, and Password in advance.

NOTE: It may be necessary to change your IP access to the local area network to match the one used by the MDS entraNET 900. (Defaults: IP–192.168.1.1, Netmask–255.255.0.0) You can identify or verify the transceiver's IP address using a terminal-emulator to communicate with the transceiver through the COM1 Port and then viewing the *Starting Information Screen*.

If you are accessing the entraNET MS via a browser connected to the LAN port, you will see a sign-in screen similar to the one shown in Figure 3-5.

Figure 3-5. Sign-in Screen when using a Web Browser

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight characters.

The following are detailed procedures for connecting to the embedded Management System.

Procedure with Terminal Emulator

a. Connect a computer's serial communications port to the transceiver's COM1 Port connector.

b. Launch a terminal emulator program, such as HyperTerminal, on the computer. Configure it to 19,200 bps data rate, 8-bit characters, no parity, one stop bit, and no flow-control. Use ANSI or VT100 emulation.

c. Press the **ENTER** key. A login screen will be displayed that requires a user name and password to access the Management System. (User = **admin**; default password = **admin**)

The radio will respond with a login screen, followed by the start-up screen similar to Figure 3-5 on Page 29.

NOTE: If the transceiver is powered-up or rebooted while connected to a terminal, you will see a series of pages of text information relating to the booting of the unit's microcomputer. Wait for the initial entraNET MS login screen before proceeding. The boot process takes approximately 30 seconds.

Procedure with Telnet (AP only)

a. Connect a personal computer's Ethernet port to the LAN Port connector on the AP transceiver using an Ethernet crossover cable or connect the AP to the network. (See Figure 2-1 on Page 14 for location.) The LAN LED will light to indicate an active connection.

b. Start the Telnet program on your computer targeting the IP address of the transceiver to which you are connected and press the **ENTER** key.

For example, in Windows: **Start>Run>Telnet**

NOTE: Do not connect multiple transceivers with the default IP address (192.168.1.1) to the network.

c. The transceiver will respond with a login screen. Enter your username and password. (Default = **admin**)

The entraNET responds with the start-up menu screen. (Figure 3-6 on Page 32)

Procedure with Web Browser (AP only)

a. Connect a personal computer's Ethernet port to the LAN Port connector on the transceiver using an Ethernet crossover cable. (See Figure 2-1 on Page 14 for location.) The LAN LED will light to indicate an active connection.

b. Launch a Web-browser on your computer.

c. Type in the radio's IP address. For example **192.168.1.1** and press the **ENTER** key. (Default address = **192.168.1.1**)

d. A login screen will be displayed that requires a user name and password to access the Management System. Note that the default entries are made in *lower case*.
(Defaults: user = **admin**; password= **admin**)

e. The transceiver responds with the startup menu screen.
(See Figure 3-6 on Page 32.)

NOTE: If the default address of 192.168.1.1 does not work, use the terminal-emulator procedure to communicate with the unit through the COM1 port. The current IP address will be displayed on the *Starting Information Screen* (Figure 3-6 on Page 32).

3.1.4 Navigating the Menus

Web Browser

Navigating with a Web browser is straightforward with a framed page. The primary navigation menu is permanently located in the left-hand window. The right-hand window displays the current menu item.

Telnet/Terminal Session

The text-based interface, accessible through Telnet or terminal emulator, uses a traditional multi-layered text menu system. To move further down a path in the menu tree, type the letter key to the left of the menu item. You will automatically move to the associated screen. In most cases, use the **ESCAPE** key to move back up a level.

In general, the top portion of screens will show read-only information with no user selection letter. The bottom portion of the screen contains parameters that can be selected for further information, alteration of values, or to navigate to other menus.

When you arrive at a screen with user-controllable parameter fields, you select the menu item by keying in an associated letter. If there is a user definable value, the field will clear to the right of the menu item and you will be allowed to type in the value you wish to use. Follow this action by the **ENTER** key to save the changes. If you make a mistake or change your mind before pressing the **ENTER** key, press **ESCAPE** to restore the previous value.

In some cases, when you type a letter to select a parameter, you will see a prompt at the bottom of the screen that says “Choose an Option.” In these cases, press the keyboard’s **SPACEBAR** to step through the available selections. When the desired option appears, press the **ENTER** key to save the selection. In some screens, several parameters may be changed and then saved by a single keystroke. The **ESCAPE** key can be used to cancel the action and restore the previous value.

3.1.5 Logging Out of the entraNET Management System

NOTE: To maintain security, it is best to formally log-out of the entraNET Management System. If you do not log out, the session will be terminated after 10 minutes of inactivity.

Via Web Browser

To logout of the entraNET MS with a Web browser, click on the "Logout" listing in the left hand frame of the browser window. The right-hand frame will change to a logout page. Follow the instructions on this Web page.

Via Telnet or Terminal Emulator

From the Main Menu, press "Q" to quit and terminate the session.

3.2 BASIC DEVICE INFORMATION

3.2.1 Starting Information Screen

Once you have logged into the entraNET Management System, you will be presented with a screen that provides an overview of the transceiver and its current operating condition.

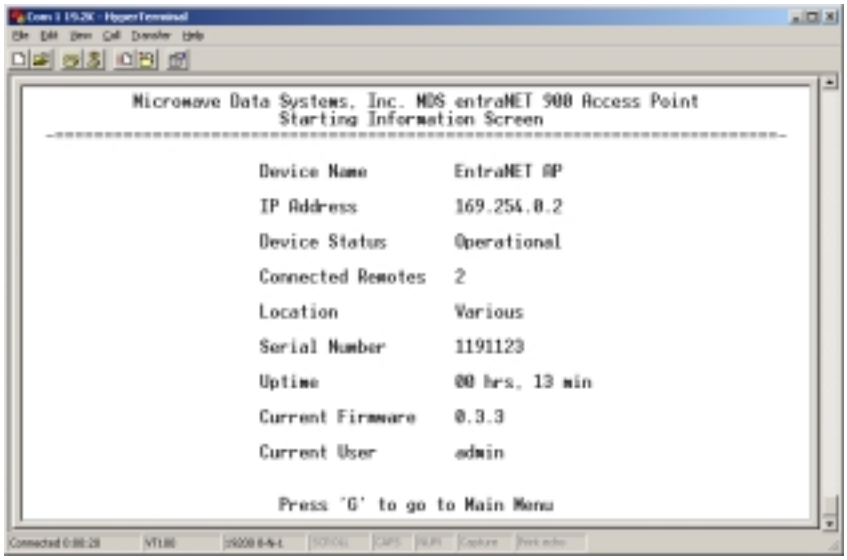


Figure 3-6. Starting Menu

- **`Device Name`**—This is a user-defined parameter that appears in the heading of all screens. (To change it, refer to *DEVICE INFORMATION MENU*, on Page 64.)
- **`IP Address`**—Shows unit's IP address.
- **`Device Status`**—Condition of transceiver as described below:
  - *Operational*—Unit operating normally.
  - *Alarmed*—A alarming event has been logged and not cleared. NOTE: If an alarm is present when this screen is dis-

played, an “A)” will appear to the left of the **Device Status** field as seen in Figure 3-6. Pressing the “A” key on your keyboard will take you directly to the “Current Alarms” screen.

- **`Connected Remotes–`** Current number of Remote radios connected to the AP.
- **`Location–`**User definable string used to help identify the unit.
- **`Serial Number`**—Unique identifier for this device. It must be provided to purchase Authorization Keys to upgrade unit capabilities. (See *“Authorization Keys Menu”* on Page 78.)
- **`Uptime`**—Elapsed time since the transceiver was powered-up.
- **`Current Firmware`**—Version of firmware that is currently active in the unit.
- **`Current User`**—Level at which the user has logged in.

3.2.2 Main Menu

The next screen, the Main Menu, is the entryway to all user-controllable features. The radio’s Device Name appears at the top of this and all other screens as a reminder of the unit that is currently being controlled.

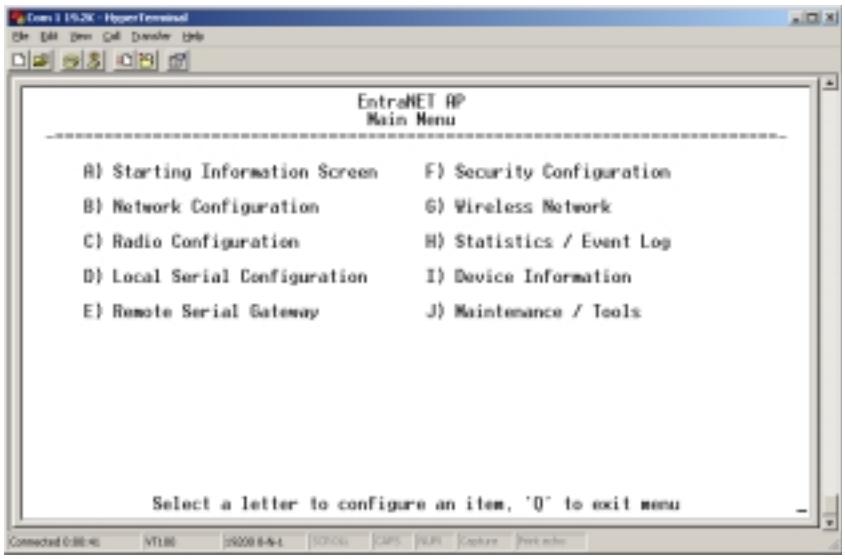


Figure 3-7. Main Menu

- **`Starting Information Screen`**—Select this item to return to the start-up screen. (See *“Starting Information Screen”* on Page 32)
- **`Network Configuration`**—Tools to configure the data network layer of the transceiver. (See *“Network Configuration Menu”* on Page 34)
- **`Radio Configuration`**—Tools to configure the wireless (radio) layer of the transceiver. (See *“Radio Configuration Menu”* on Page 40)

- **Local Serial Configuration**—Tools to configure the COM1 and COM2 serial port of the AP. (See *"Serial Data Port Configuration Menu (Local Serial-to-Remote Serial or IP-to-Local Serial)"* on Page 44)
- **Remote Serial Gateway**—Contains tools to configure data connections to the Remote transceiver serial ports.
- **Security Configuration**—Tools to configure the security services available with the transceiver environment. (See *"SECURITY CONFIGURATION"* on Page 49)
- **Wireless Network**—Tools to manage Remote and Access Point databases, and manage Remote radios. (See *"WIRELESS NETWORK MENU"* **on Page 51**
- **Statistics/Event Log**—Tools to measure the radio and data layer's performance of the network. (See *"STATISTICS/EVENT LOG"* on Page 56)
- **Device Information**—Top level user-specific and definable parameters, such as unit password. (See *"DEVICE INFORMATION MENU"* on Page 64)
- **Maintenance/Tools**—Tools to use configuration files, change firmware and use Authorization Keys to change major unit capabilities. (See *"MAINTENANCE/TOOLS"* on Page 65)

3.3 CONFIGURING NETWORK PARAMETERS

3.3.1 Network Configuration Menu

The *Network Configuration Menu* (Figure 3-8) is the home of all IP and Ethernet level parameters.

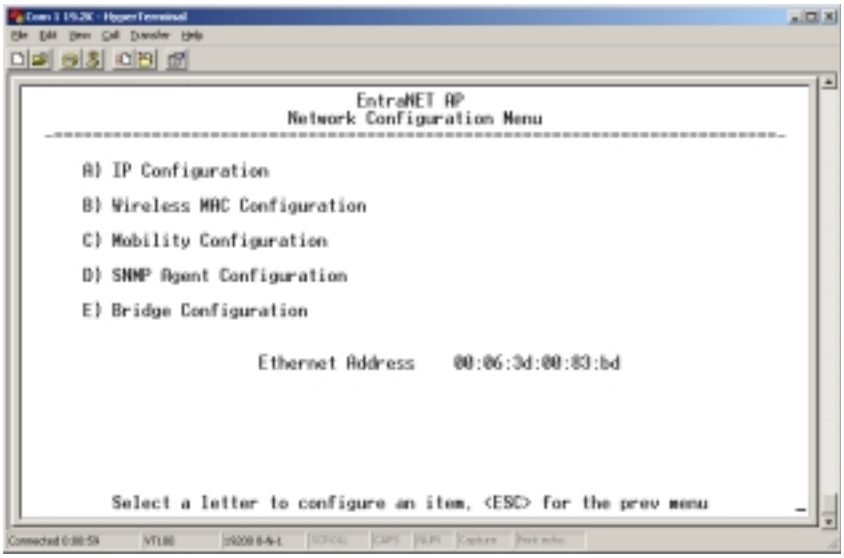


Figure 3-8. Network Configuration Menu
From Access Point

This menu is subdivided into six sections as follows:

- **IP Configuration**—The transceiver's IP address and similar parameters.
- **Wireless MAC Configuration**—Parameters for the Media Access Control (MAC)wireless protocol.
- **Mobility Configuration**—Parameters that govern the behavior of handoffs.
- **SNMP Configuration** *(Available soon)*—Details that control the operation of SNMP.
- **Bridge Configuration**—Specialized parameters for operation of Ethernet bridging, including priority and forward delay.
- **Ethernet Address**—Shows the Ethernet Address of the local unit.

3.3.2 IP Configuration Menu

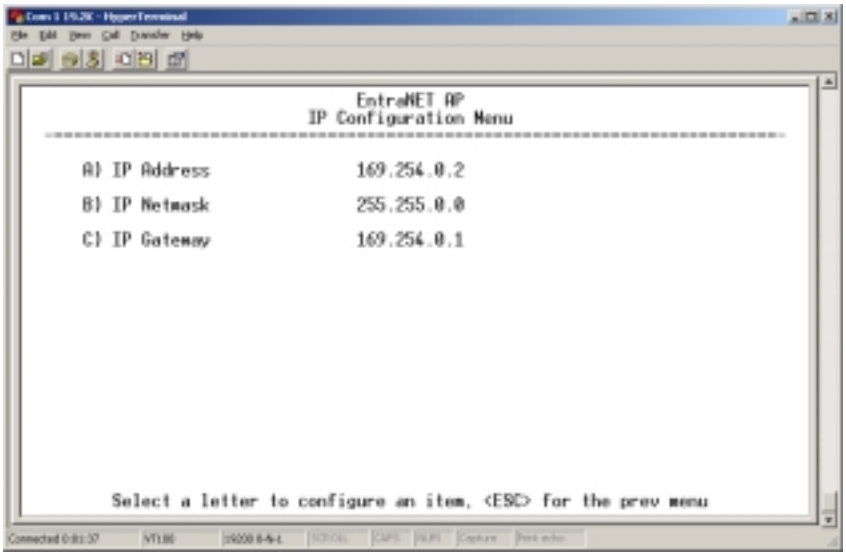


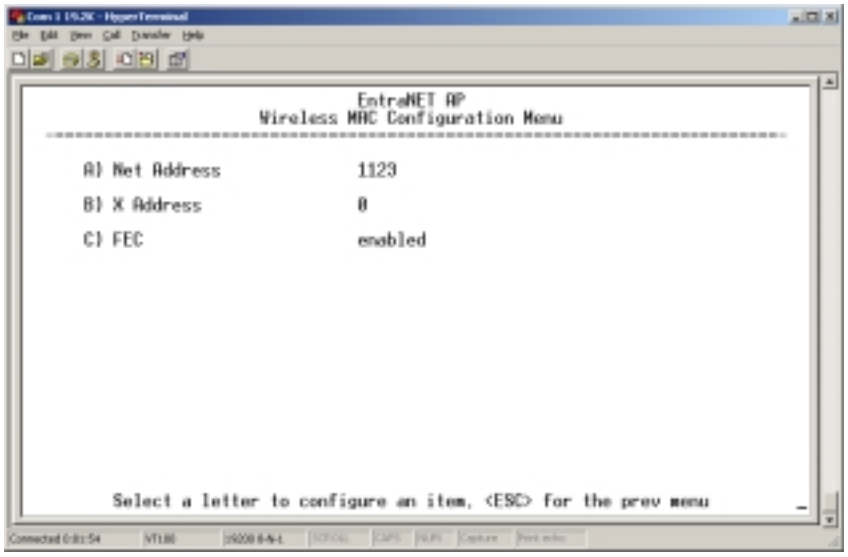
Figure 3-9. IP Configuration Menu

- **`IP Address`** *(User Review Recommended)*—Essential for connectivity to the MDS entraNET 900 MS via the LAN port and over the air. Enter any valid IP address that will be unique within the network. [192.168.1.1]

  CAUTION: Changing this value in the transceiver while you are communicating with it over the network, will cause a loss of communication with the transceiver. Communication will need to be re-established using the new IP address.
- **`IP Netmask`**—The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [255.255.0.0]
- **`IP Gateway`**—The IPv4 address of the default gateway device, typically a router. This field is unnecessary if all devices are on the same subnet [0.0.0.0]

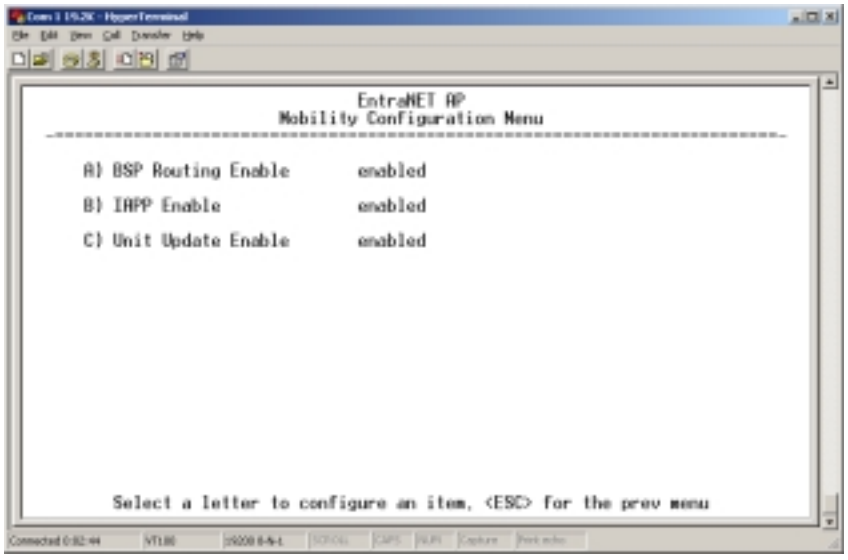
NOTE: The radio is not a router, and thus all IP parameters are used to gain access to local management only, and has no affect on the routing of data.

3.3.3 Wireless MAC Configuration



- **`Radio Net(work) Address`** *(User Review Required)*—ID of the network of which this unit will be a part. Essential for connection of Remotes to the Access Point in the entraNET network. [Not Programmed]
- **`X Address`**—"Extended Address" used for store and forward operation and in installations with multiple APs supporting mobility. Net Address and X Address pairs must be unique. For single AP networks, this parameter is not used.
- **FEC**—Forward Error Correction status (enabled/disabled)

3.3.4 Mobility Configuration Menu



- **BSP Routing Enable**—This parameter enables intra-cell and routing of Basic Serial Protocol packets.
- **IAPP Enable**—This parameter enables Inter-Access Point Protocol which allows Access Points to pass payload data over the Ethernet LAN.
- **Unit Update Enable**—This parameter allows the Access Point to immediately send out an IAPP update when a Remote connects or disconnects.

SNMP Configuration (Figure 3-10)

The current release of transceiver firmware does not support SNMP management. This functionality is planned for a future release of the product. The following descriptions are supplied to support future SNMP functionality.

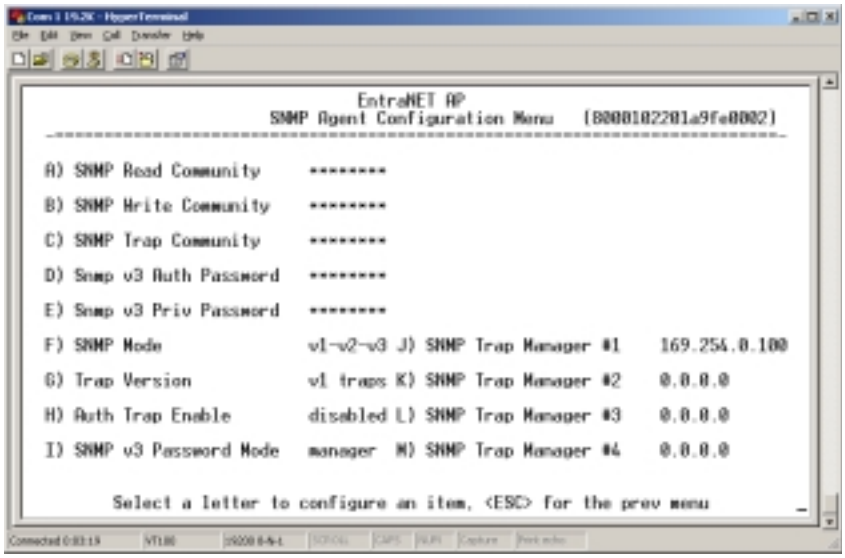


Figure 3-10. SNMP Agent Configuration Menu

This menu provides configuration and control of vital SNMP functions.

- **Read community**—Community name with SNMP read-level access. Any 30-character alphanumeric string.
- **Write community**—Community name with SNMP write-level access. Any 30-character alphanumeric string.
- **Trap community**—Community name with SNMP access to receive traps. Any 30-character alphanumeric string.
- **SNMP v3 Password**—Determines whether v3 passwords are managed locally or via an SNMP Manager. The different behaviors of the Agent, depending on the mode selected, are described in **SNMP Mode** below. [Manager, Local; Local]

- **SNMP v3 Priv Password**—Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 used for privacy (DES encryption). The password string can be between 8 and 30 alpha-numeric characters. [Manager, Local; Local]
- **SNMP Mode**—Current state of the SNMP agent. [Enable/Disabled, v1-only, v2-only, v3-only, v3-only, v1-v2, v1-v2-v3; Disabled]
- **Trap Version**—Set version to be used with traps. [v1 Traps, v2 Traps]
- **Auth Trap Enable**—Current state of the authentication traps. [Disabled/Enabled; Disabled]
- **Trap Manager (#1–#4)**— Table of up to 4 locations that traps are sent to. (Any standard IP address)

3.3.5 Bridge Configuration Menu

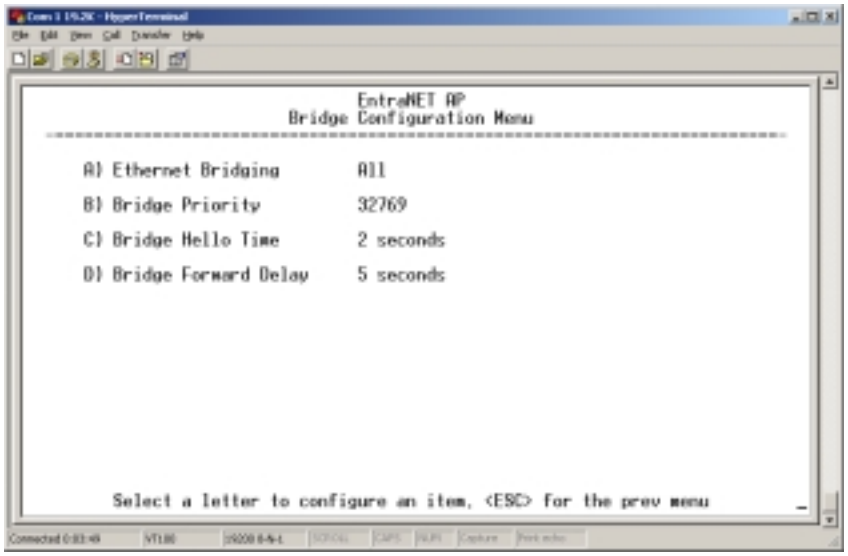


Figure 3-11. Bridge Configuration Menu

- **Ethernet Bridging**—Allows choice as to packets sent over bridge.
- **Bridge Priority**—This value is used along with the MAC address to define the bridge ID. The Bridge ID is used by the Spanning Tree protocol to determine the root bridge in the network. This value is useful for forcing a certain bridge to always be the root.
- **Bridge Hello Time**—Defines how often Spanning Tree protocol Bridge Protocol Data Units (BPDU) are sent out by the Access Point. Each bridge in the network should have the same hello time.

- **`Bridge Forward Delay`**—This value decides how long a bridge will spend in the “learning” and “listening” states. Traffic will begin forwarding through the bridge after 2 * Forward Delay.

3.4 CONFIGURING RADIO PARAMETERS

There are two primary data layers in the MDS entraNET 900 network—radio and data. The data layer is dependent on the radio layer to work properly. The *Radio Configuration Menu*, is the primary radio menu. There is also a secondary menu, the *Skip Zone Options Menu*.

3.4.1 Radio Configuration Menu

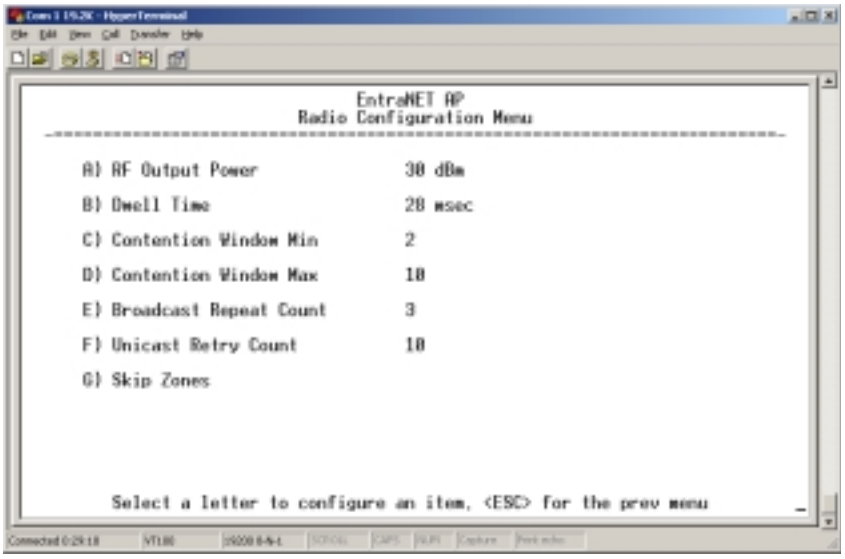


Figure 3-12. Radio Configuration Menu
From Access Point

- **`RF Output Power`** *(User Review Recommended)*—Set RF power output level. Displayed in dBm. Setting should reflect local regulatory limitations and losses in antenna transmission line. (See *“How Much Output Power Can be Used?”* on Page 111 for information on how to calculate this value.) [20–30; 30]
- **`Dwell Time`**—Duration of one hop on a particular frequency in the hopping pattern. **Hop Time** may be set to either 7 or 28 msec. (This field is only changeable on an Access Point. Remotes get their value from AP upon association.) [7,28 msec; 7 msec]
- **`Contention Window Min`**—Sets number of random contention slots to use on first attempt.
- **`Contention Window Max`**—Sets the *maximum* number of random contention slots to use.

- **`Broadcast Repeat Count`**—Sets the number of times point-to-multipoint messages will be transmitted by the AP. Higher values provide more reliability but also more over-the-air congestion.
- **`Unicast Retry Count`**—Sets the *maximum* number of attempts that will be made to deliver point-to-point messages.Higher values provide more reliability but also more over-the-air congestion.
- **`Skip Zones`** *(Editable at Access Point Only)*—Display of current utilization of zones. Each zone consists of 16 RF channels. (See *"Skip Zone Options Menu"* on Page 41.)

Skip Zone Options Menu

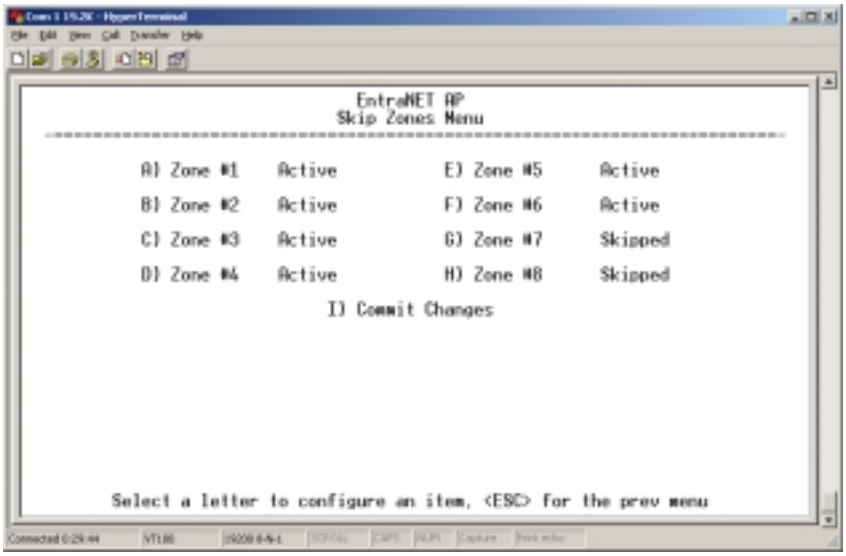


Figure 3-13. Skip Zones Menu
("Commit changes" displayed only on Access Point units)

This is a display of current utilization of 8 frequency operating zones. Zones can be toggled between **Active** and **Skipped** at Access Point units by first keying in the letter of the zone to be changed, and then pressing the spacebar to toggle between the two options for each zone. Select the **Commit Changes** menu item to implement changes. These changes will be forwarded to all units in the network through the Access Point's beacon signal.

In the USA, a maximum of four zones can be skipped and still be compliant with FCC regulations.

3.5 CONFIGURING THE SERIAL INTERFACES

3.5.1 Overview

To understand the operation of the radio system, it may be helpful to visualize the AP and the Remotes as being in a single box, with the AP ports on one side and all of the Remotes on the other (see Figure 3-14). In practice, the units are typically separated by considerable distances, but viewing them as a single unit will be helpful for this discussion.

Most system processing is done at the AP, and thus, majority of the configuration for the Remote units must also be performed at the AP. The AP requires configuration of its local interfaces (Ethernet or Serial) and its remote interfaces—the latter being physically located at the Remote radios. A few parameters must also be configured at the individual Remote units.

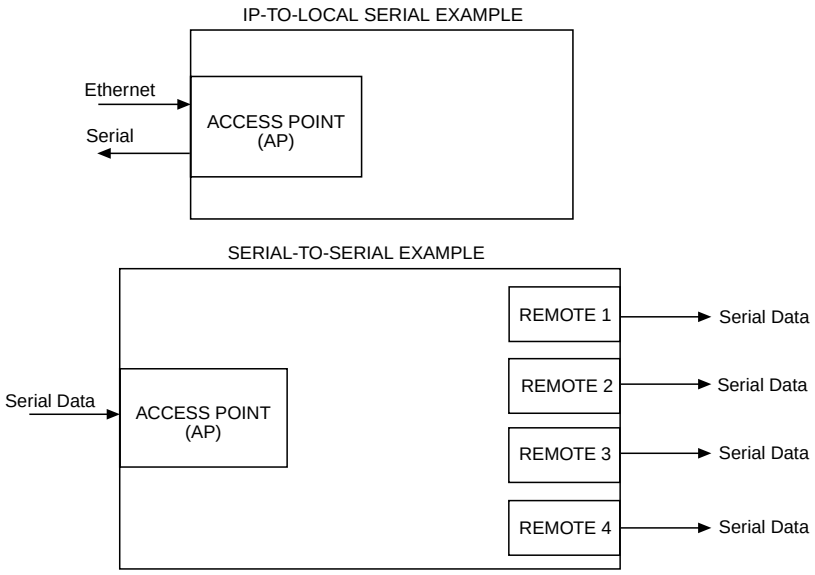


Figure 3-14. Conceptual Views of Radio System

The AP includes an embedded terminal server that provides access to Remote serial ports via an IP or serial connection at the AP. In this capacity, it acts as a gateway between IP and Remote serial devices (thus the name “Serial Gateway), or a transparent over-the-air serial-to-serial connection.

IP-to-Serial Services

When the AP transceiver is used as an IP-to-serial gateway, two types of IP terminal services are possible—TCP and UDP. TCP provides a connection-oriented link, with end-to-end acknowledgment of data, but with some added overhead. UDP provides a best-effort delivery service with less overhead than TCP.

To configure IP-to-remote serial services, use the Remote Serial Gateway menu (Figure 3-20 on Page 48). To configure local serial-to-remote-serial *or* IP-to-local-serial services, use the Local Serial Configuration menu Figure 3-15 on Page 44.

Most polled protocols will be best served by UDP services as the protocol itself has built-in recovery mechanisms (error-correction). UDP provides the needed multidrop operation by means of multicast addressing, where multiple remote devices will receive and process the same poll message. The serial-to-serial example which follows, shows how to provide multicast services. (See *"Point-to-Multipoint Serial-to-Serial Application Example"* on Page 100.)

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism (error-correction) and most have the guaranteed delivery that TCP provides despite the extra overhead. The IP-to-Serial example shows how to do this. (See *"IP-to-Local Serial Application Example"* on Page 97.)

Configuration

There are several configuration parameters for the Remote Serial Gateway found under the *Serial Configuration Menu* of the entraNET Management System. Note that some of the parameters are not applicable to IP-to-Serial mode. After making changes to the configuration, you must use the menu's "Execute Changes" to cause the transceiver to implement the requested changes.

If you are connecting EIA-232 serial devices to the transceiver, review these parameters carefully.

Serial Configuration Wizard

The Serial Configuration Wizard available through the **Serial Data Port Configuration Menu** is recommended for configuration of serial ports. The wizard uses a step-by-step process that eliminates possible conflicting settings, and streamlines complex configurations.

3.5.2 Serial Data Port Configuration Menu
(Local Serial-to-Remote Serial, or IP-to-Local Serial)

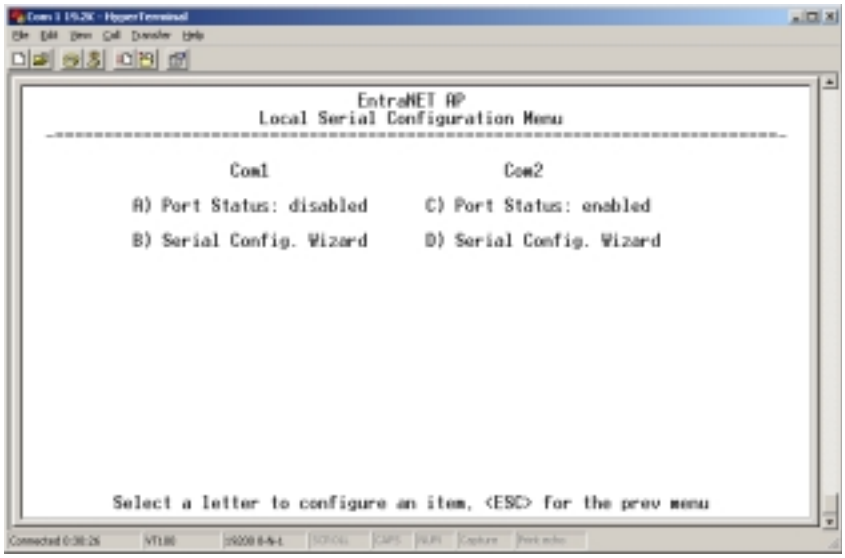


Figure 3-15. COM1/2—Local Serial Configuration Menu

- **`Port Status`**—Defines whether the serial COM1/2 port is enabled or disabled to pass data.
- **`Serial Configuration Wizard`**—Tool for configuration of the serial ports using a step-by-step process. When the wizard is started, you may choose between beginning the step-by-step process, or simply viewing the current settings (see Figure 3-16).

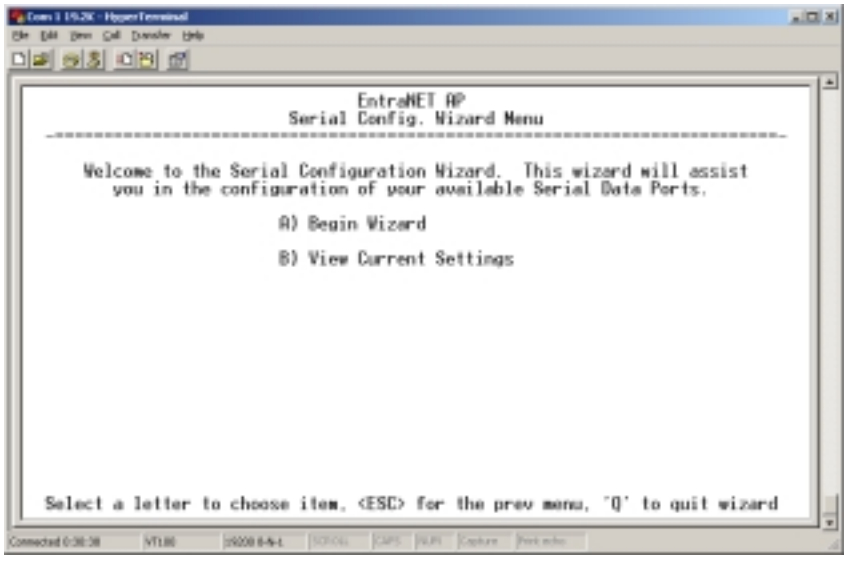


Figure 3-16. Serial Configuration Wizard (Starting Screen)

The Serial Configuration Wizard consists of a series of screens used to set all of the parameters needed for proper operation of the serial port(s). Each screen provides text that will help you in choosing selections.

If you choose “View Current Settings,” you will see a summary screen of the serial configuration settings (Figure 3-17). Here, you may either select the letter of an item to change, or exit the configuration wizard.

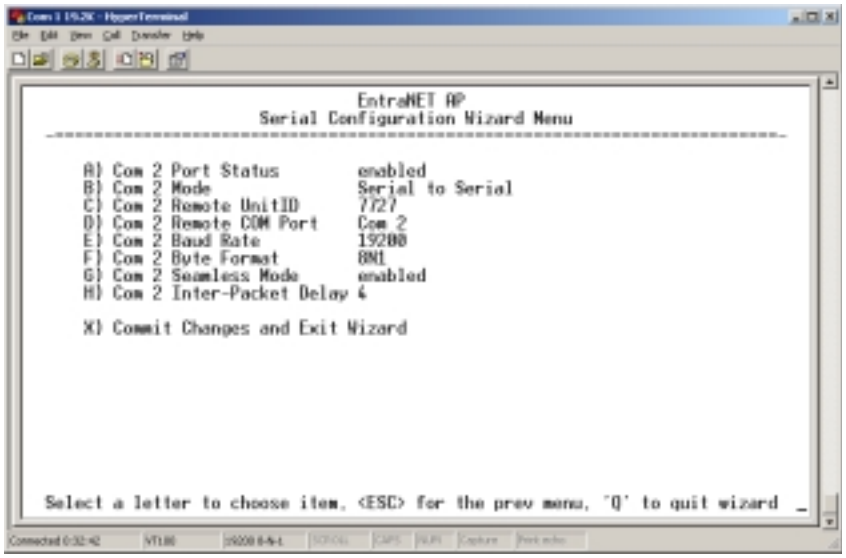


Figure 3-17. Serial Configuration Wizard Summary Screen *(Serial-to-Serial example)*

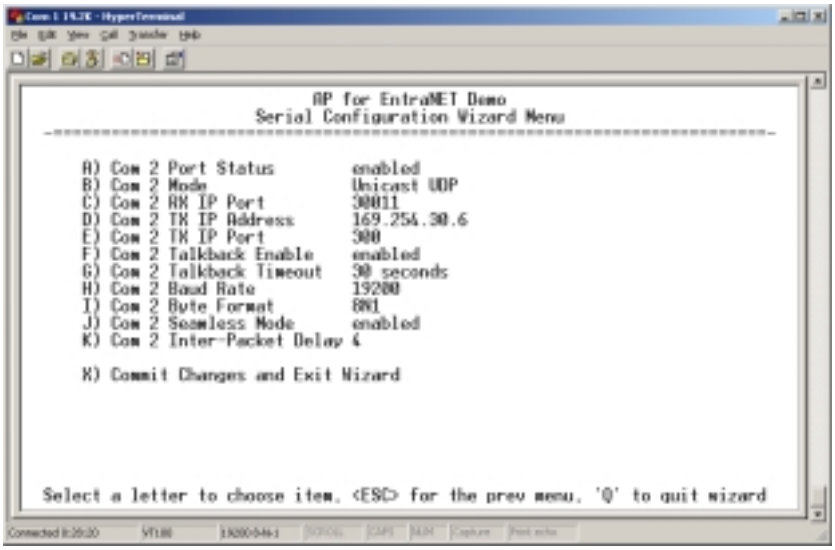


Figure 3-18. Serial Configuration Wizard Summary Screen *(IP-to-Serial Example)*

The following text explains the key settings for the serial configuration menus.

- **Port Status**—Enable/Disable the serial data port.

NOTE: Setting the COM1 port to **Enable** prevents access of the entraNET Management System (MS) through this port. However, the entraNET MS can still be accessed via Telnet or browser through the LAN port.

To restore the COM1 port to support Management System access, connect a terminal to the port and enter an escape sequence to reset it the console mode. (**+++ ENTER**)

- **Mode**—Serial-to-Serial, TCP (IP-to-Serial), UDP (IP-to-Serial).
- **Remote UnitID**—"Broadcast" or Unit ID of Remote for unicast (directed) data.
- **Remote COM Port**—Remote's serial port (COM1 or COM2 with which to exchange data.
- **Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1,200–115,200; 19200]
- **Byte Format**—Interface signaling parameters. Data bits, parity and stop bits.
  [7N1, 7E1, 7O1, 8N1, 8E1, 8O1; 8N1]
- **Seamless Mode**—Seamless mode accommodates protocols that do not tolerate gaps in the middle of a frame (e.g., MODBUS™ ASCII). In these protocols, gaps are interpreted by the connected device as an "end-of-frame" indication, which may cause errors.Seamless mode resolves this problem through the use of buffers.

  When Seamless mode is enabled, the buffer is set to 256 bytes. Data bytes are sent over the air as soon as they are received at the local serial port. At the other end of the link, the receiving radio buffers incoming data until enough characters have been received to cover the worst case (longest) gaps in transmission. (These generally occur during over-the-air retries.) This ensures a continuous stream of data will be delivered out the remote end's serial port and to the connected device.

  When Seamless mode is disabled, the buffer size is set to the last value set in the custom buffer parameter. [Enabled, Disabled; Disabled]

NOTE: Seamless mode is intended only for applications where the transmitter's baud rate is greater than or equal to the receiver's baud rate. Enforcement of this rule is left up to the user.

- **`Inter-Packet Delay`**— Number of characters that represent the end of a message (inter-character time-out). A transceiver receiving data through the serial port will send an end-of-message signal to the remote end. MODBUS defines a “3.5-character” parameter. [0–1,000; 0]

3.5.3 Remote Serial Gateway Configuration *(IP-to-Remote Serial)*

The serial gateway controls the behavior of all Remote radios from the perspective of IP encapsulation. The gateway is basically a table with one entry for each Serial Remote radio. Ethernet radios are not defined in the serial gateway. No further configuration is required at the Remote radios.

The AP can be configured to accept IP traffic to be exchanged with devices connected to the serial ports of one or more Remotes. Figure 3-19 shows the starting point for configuring the Remote Serial Gateway settings.

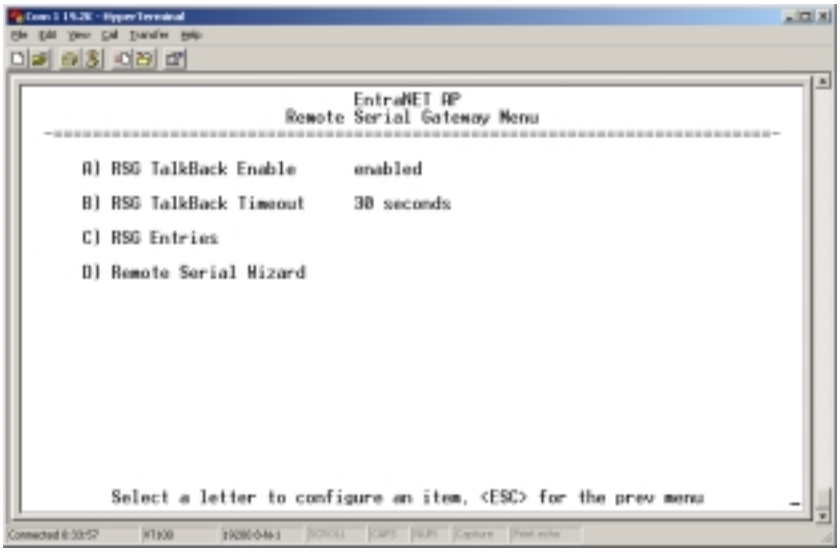


Figure 3-19. Serial Configuration for Remote Radios

- **`RSG Talkback Enable`** (UDP IP-to-Serial)—When this option is enabled, and the RSG is set up for UDP mode, a message from a Remote radio (usually a reply to a poll) will be sent to the last IP address/port that a message was received from.
- **`RSG Talkback Timeout`**—After this timeout has expired (time since the last data has been received from an IP

host) the RSG will revert to its configured IP address and port for upstream data destined for an IP host.

- **RSG Entries**—Allows entry of key RSG parameters including Unit ID, COM Port setting, Mode, and Local IP Port selection. This screen is shown in Figure 3-20.
- **Remote Serial Wizard**—Tool that will assist you in adding/changing a configuration to your Remote Serial Gateway entries.

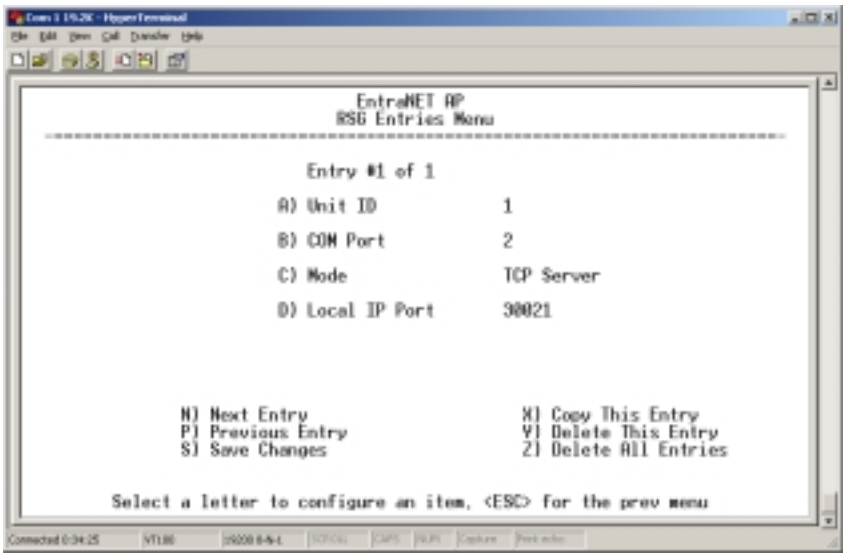


Figure 3-20. Remote Serial Gateway (RSG) Entries Menu
(TCP Configuration Example, UDP Similar)

- **Unit ID**—"Broadcast" or the Unit ID of Remote for unicast (directed data.
- **COM Port**—Remote's serial port with which to exchange data.
- **Mode**—TCP server or UDP.
- **Local IP Port**—The IP Port Number to which an application will connect to exchange data via the AP.

3.6 SECURITY CONFIGURATION

There are many options for assisting you in providing secondary security for your transceivers and the network. These options start with controlling remote access to the network via Telnet, Web Browser, and SNMP. Other areas include multiple levels of encryption and MD5-level security for HTTP connections.

3.6.1 Security Configuration Menu

The Security Configuration Menu (Figure 3-21) allows settings of several parameters related to network access, user credentials, and encryption. A review of each item on the menu is important to safeguarding your network from unauthorized access. These settings should be reviewed from time to time to make sure they are applicable to the current state of your network.

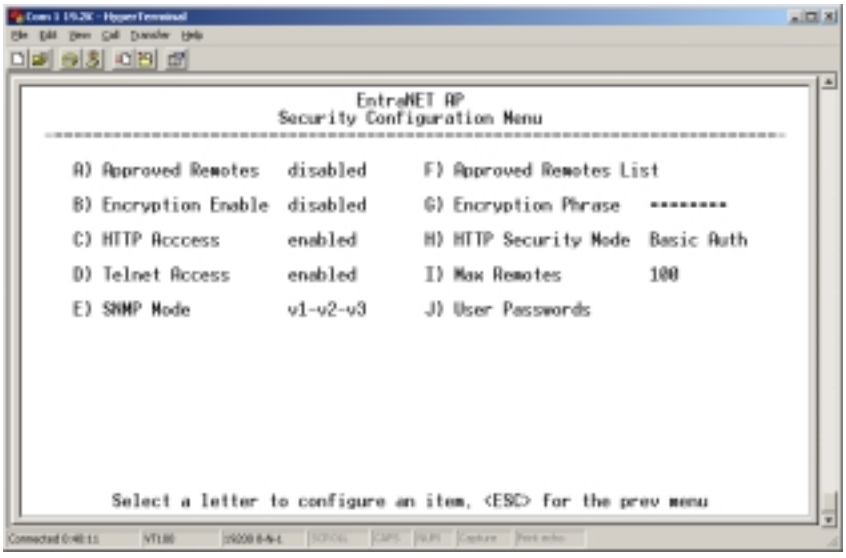


Figure 3-21. Security Configuration Menu

- **`Approved Remotes`**— Enables authentication of Remote radios before granting access to the network. [Enabled/Disabled; Disabled]

  Enabling forces the entraNET 900 to check the *Approved Remotes List* before continuing the authorization process. Before enabling this option, at least one entry must already exist in the *Approved Remotes List*.
- **`Encryption Enable`**— Enable encryption of over-the-air data packets. [Enabled, Disabled; Disabled]

  Enabling forces the transceiver to use 128-bit encryption on all over-the-air messages. This option requires the Encryption Phrase to be previously configured.

- **HTTP Access**—Prevents remote access through HTTP (Web browser) on Port 80 [Enabled/Disabled; Disabled]
- **Telnet Access**—Prevents remote access through Telnet sessions on Port 23 [Enabled, Disabled; Enabled]
- **SNMP Mode**— Prevents remote access through SNMP commands on Port 161 [Enabled, Disabled; Enabled]
- **Approved Remotes List (Menu)**—Presents a menu where the creation and management of Remote units allowed to communicate with the AP is performed.
- **Encryption Phrase**—Phrase (text & numbers) that will be part of the encryption algorithm. [Any 30-character alphanumeric string; Blank]
- **HTTP Security Mode**—Select security mode/level of login via HTTP browser. **HTTP Access** disabled prevents access through HTTP. **HTTP Security Mode** is functional if **HTTP Access** is enabled. [Basic Auth, MD5 Digest; Basic Auth]

  Basic mode requires a password, but the actual password text is transmitted in the clear (unencrypted).

  MD5 is the most secure mode. MD5 Digest protects/encrypts the password and is supported by recent releases of many browsers.
- **Max Remotes**—Maximum number of Remotes permitted to be connected with (served by) this Access Point. [Default=50]
- **User Password**—General administrative password only for this unit. Used at log-in via COM1 Port, Telnet and Web browser. [Up to 8-character alphanumeric string without spaces (case-sensitive); Default=**admin**]

TIP: For enhanced security, consider using a misspelled word. This helps protect against sophisticated hackers who may use a database of common words (e.g., dictionary attack) to determine a password. An even better approach is to use a password that includes some numbers inter-mixed with letters. Making the password as long as possible (up to the full 8 characters) will also improve its security.

3.6.2 Approved Remotes List Menu

The Access Point restricts communication to only those Remotes included in the Approved Remotes List. Messages received from Remotes that are not in this list are discarded.

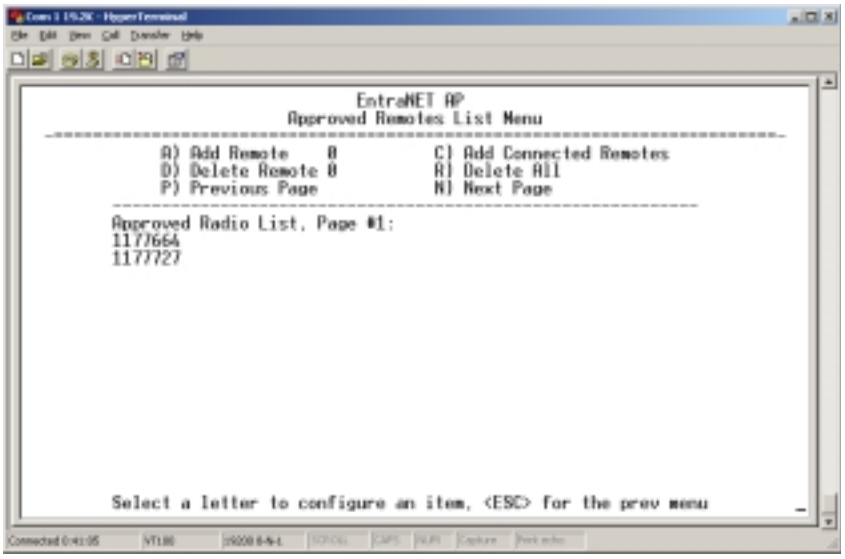


Figure 3-22. Approved Remotes List Menu

- **`Add Remote`**—Enter the serial number of Remote. [ten-digit number]
- **`Delete Remote`**—Enter serial number of Remote to be deleted.

  For security purposes, you should delete a deprovisioned or stolen radio.
- **`Previous Page`**—Returns you to the last page viewed within the Approved Remotes Menu.
- **`Add Connected Remotes`**—Adds all currently connected Remotes (1-255) to the approved Remote list. Alternatively, you can enter each Remote serial number manually.
- **`Delete All`**—Remove (complete purge) of all Remotes from current list.
- **`Next Page`**—Moves you to the next page within the Approved Remotes Menu.
- **`Approved Radio List`**—Simple listing of Remotes by serial number, that are authorized to communicate this AP. If a Remote is not in this list, it will not be able to associate with this AP.
- **`Save Changes`**—Saves all changes made during this session with this menu. Changes will be implemented only if they are “saved” before exiting this menu.

3.7 WIRELESS NETWORK MENU

The Wireless Network Menu (Figure 3-23) monitors the operation of Remote radios in the network, regardless of their type (Ethernet or Serial) from the perspective of the Access Point. This information,

which is related to Remotes, is not actually sent to Remotes, but is stored in a local database at the AP.

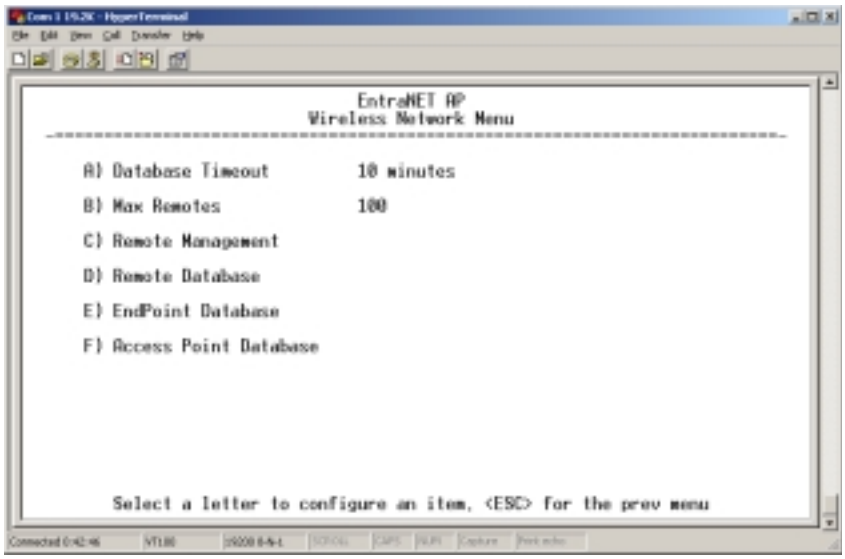


Figure 3-23. Wireless Network Menu

- **`Database Timeout`**—The time, in minutes, before a database entry expires. Remotes must be "refreshed" through a handshake process to stay in the database of connected Remotes. This allows decommissioned or faulty radios to fall out of the database to maximize efficiency if the entries are not needed. [1-720; 5]
- **`Max Remotes`**—Maximum number of Remotes allowed to associate with the AP. [1-1024;50]
- **`Remote Management`**—Presents a menu for management of a particular Remote.
- **`Remote Database`**—A listing of all Remotes connected with the AP.
- **`Endpoint Database`**—A listing of Ethernet endpoints connected via Remote radios.
- **`Access Point Database`**—A listing of Access Points in the wireless network. Inter-Access Point Protocol (IAPP) traffic can be passed via these transceivers.

Remote Management Menu

The Remote Management Menu (Figure 3-24) allows selection of a particular Remote to Manage, based on the unit's ID number.

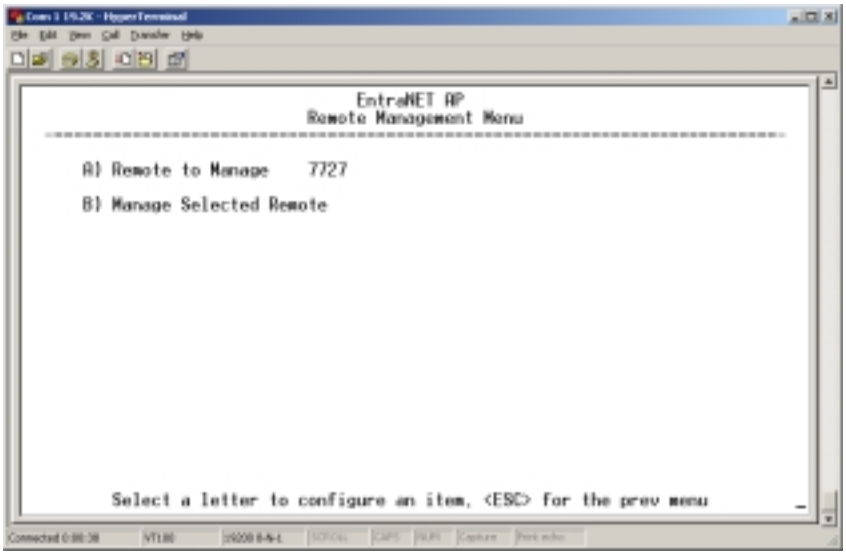


Figure 3-24. Remote Management Menu

When “Manage Selected Remote” is chosen, the screen shown in Figure 3-25 appears. It contains several items that are used to set the characteristics of Remote radios in the network.

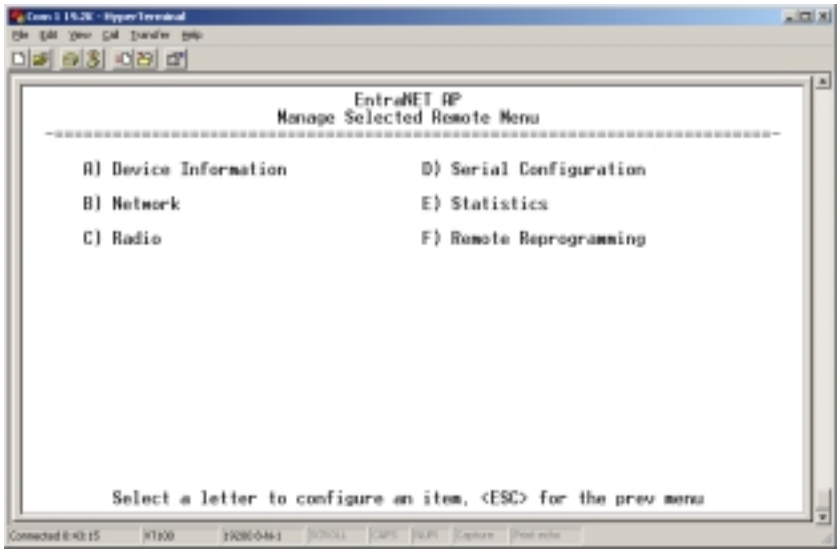


Figure 3-25. Manage Selected Remote Menu

- **`Device Information`**—Shows hardware and software version information, including bootloader version.
- **`Network`**—Tool for control of the Ethernet port (enable/disable).
- **`Radio`**—Tool for setting the radio’s transmit power level (in dBm).

- **Serial Configuration**—Tool for configuring COM1/2 parameters, including: Port Mode, Baud Rate, Byte Format, Seamless Mode, Interpacket Delay, and Buffer Size.
- **Statistic**s—Presents packet throughput and retry data for the selected Remote
- **Remote Reprogramming**—Menu for sending new firmware images and specifying the image that will be active upon re-boot.

Remote Database Menu

The Remote Database Menu (Figure 3-26) shows several parameters related to the connected Remotes. is continuously updated at a refresh rate of approximately 8 seconds.

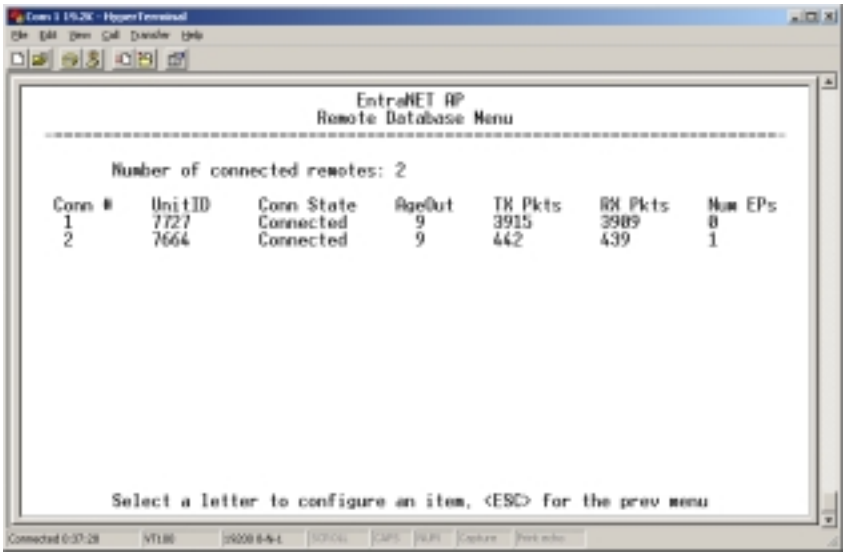


Figure 3-26. Remote Database

- **UnitID**—The unit ID of the connected Remote.
- **Conn State**—Shows whether or not the Remote is connected with the AP.
- **AgeOut**—Number of minutes before the entry ages out and is removed from the table. Each AP maintains a table with the addresses of the devices it communicates with. The AgeOut countdown is restarted to its default setting every time a message to/from that device is detected. If no traffic with that device occurs, and it does not respond to a final handshake request, it then “ages out” of the table.

  An aged out Remote must reconnect before it is again included in the table. (See “database timeout” on the Wireless Network Menu, Figure 3-23 on Page 52.
- **TX Pkts**—Number of packets sent to this Remote.

- **RX Pkts**—Number of packets received from this Remote.
- **Num EPs**—Number of endpoints connected to this Remote.

Endpoint Database Menu

The Endpoint Database Menu (Figure 3-27) shows all non-entraNET 900 Ethernet devices that are known to the transceiver and is equivalent to the ARP table of IP devices. The list shows endpoint MAC and IP addresses, as well as packet exchange data.

NOTE: An Ethernet Remote does not have an IP address; rather, it acts as a "transparent bridge" for IP traffic to the connected Ethernet endpoint.

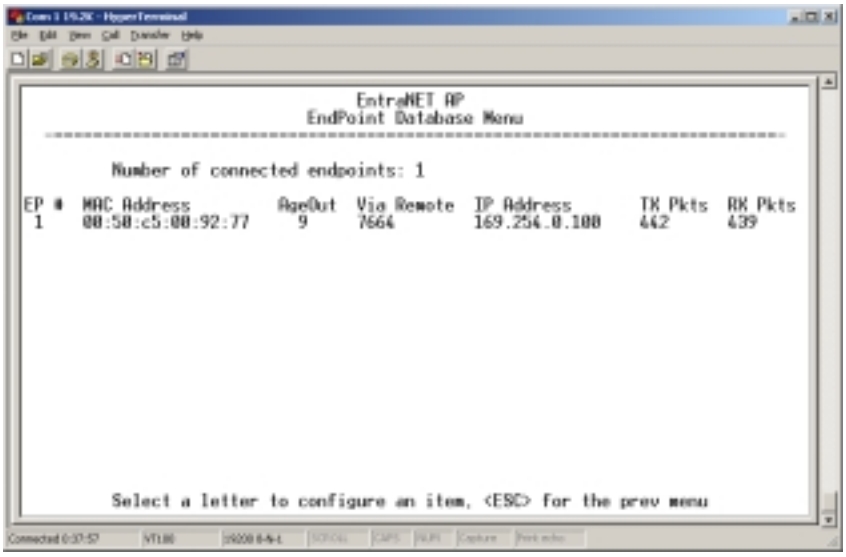


Figure 3-27. Endpoint Database
(Lists all equipment attached to REMOTE transceivers in the network)

- **MAC Address**—Ethernet address of the endpoint device.
- **AgeOut**—Time, in minutes, remaining before the device (address) will be removed from the table.

  Each transceiver maintains a table with the addresses of the devices it communicates with. The age time countdown is restarted to its default setting every time a message to/from that device is detected. If no traffic with that device happens, it then "ages out" of the table. When traffic is detected it is included again in the table.
- **Via Remote**—Unit ID of the transceiver connected to this device.
- **IP Address**—IP Address of endpoint device (not the Remote).
- **TxPkt**—Number of packets received from the endpoint device and passed over-the-air.

- **RxPkts**—Over-the-air data packets received by the transceiver. and passed on to the endpoint device.

Access Point Database Menu

The Access Point Database Menu (Figure 3-28) provides a listing of all Access Points contained in the wireless network and includes details about each unit.

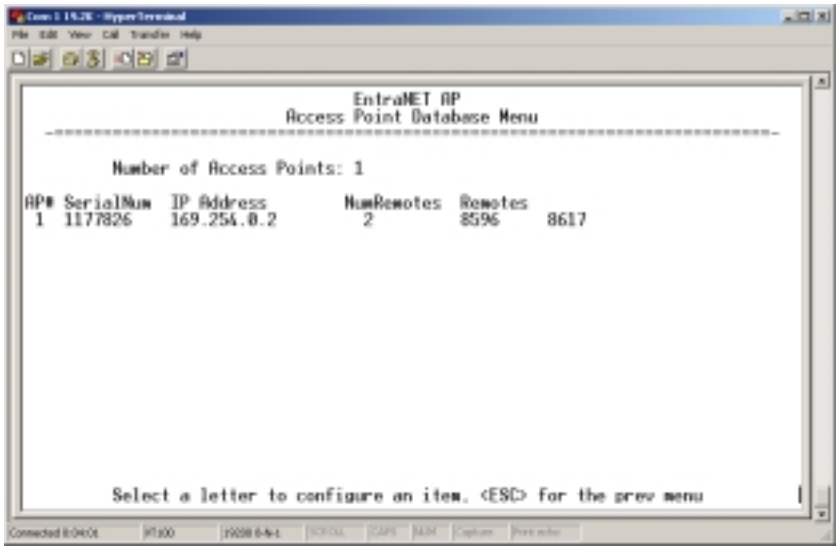


Figure 3-28. Access Point Database

- Serial Number—Factory-assigned serial number for the Access Point.
- IP Address—IP Address of the Access Point.
- Number of Remotes—Current number of Remotes connected to the Access Point.
- List of Remotes—Lists all Remotes (by Unit ID number) that are currently connected to the Access Point.

3.8 STATISTICS/EVENT LOG

The Statistics/Event Log Menu (Figure 3-29) contains a variety of items related to the health and performance of the wireless network. Data throughput statistics, as well as past/present Events and Alarms are all presented and stored in this menu area.

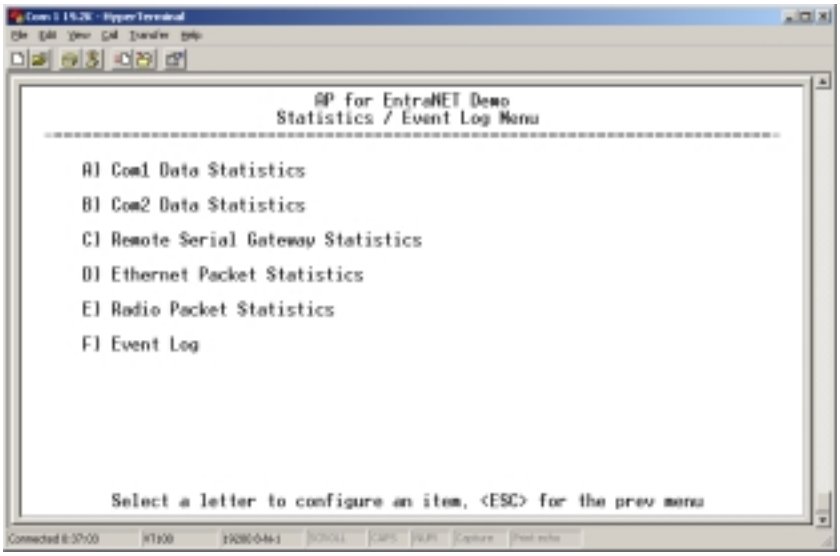


Figure 3-29. Statistics/Event Log Menu (Main Screen)

- **COM1/2 Serial Data Statistics**—These screens show bytes in/out for the COM1/2 ports
- **Remote Serial Gateway Statistics**—Shows Unit ID, status and throughput data for connected Remotes.
- **Ethernet/Wireless Packet Statistics**—Shows vital data on packets and bytes in/out of the radio, errors detected, and lost Ethernet carriers.
- **Radio Packet Statistics**—Shows a summary of data packets sent/received by the radio, including overflows, good/failed data, retries and timeouts.
- **Event Log**—Database of past and present Events and Alarms for the wireless network.

3.8.1 COM1 & 2 Serial Data Statistics Menus

(See Figure 3-30)

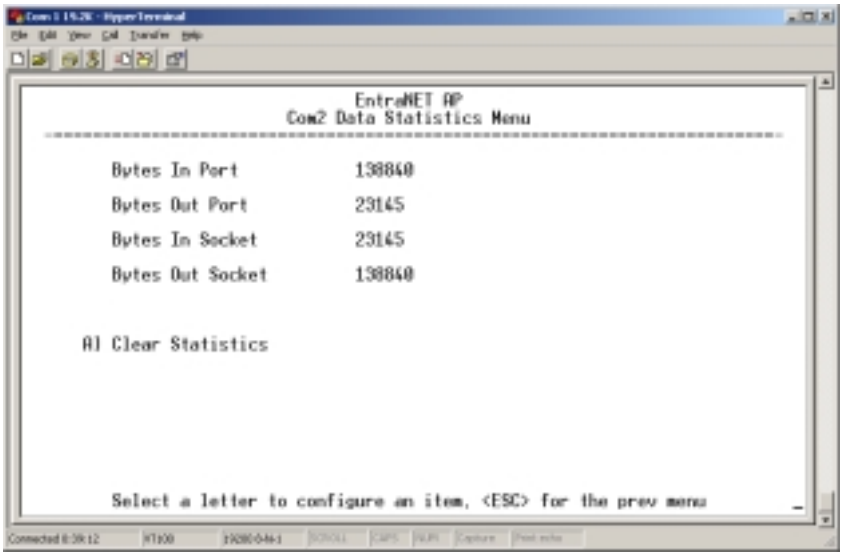


Figure 3-30. Com1/2 Data Statistics Menu

- **`Bytes in on port`—**Number of bytes received by the transceiver through the serial interface
- **`Bytes out on port`—**Number of bytes transmitted by the transceiver through the serial interface
- **`Bytes in on socket`—**Number of bytes received by the transceiver through the IP socket
- **`Bytes out on socket`—**Number of bytes transmitted by the transceiver through the IP socket.

3.8.2 Remote Serial Gateway Statistics Menu

(See Figure 3-31)

This screen provides a summary of port activity for Remote Serial Gateway entries that have been set up for IP-to-remote serial data. These values will be reset to zero after a reboot cycle.

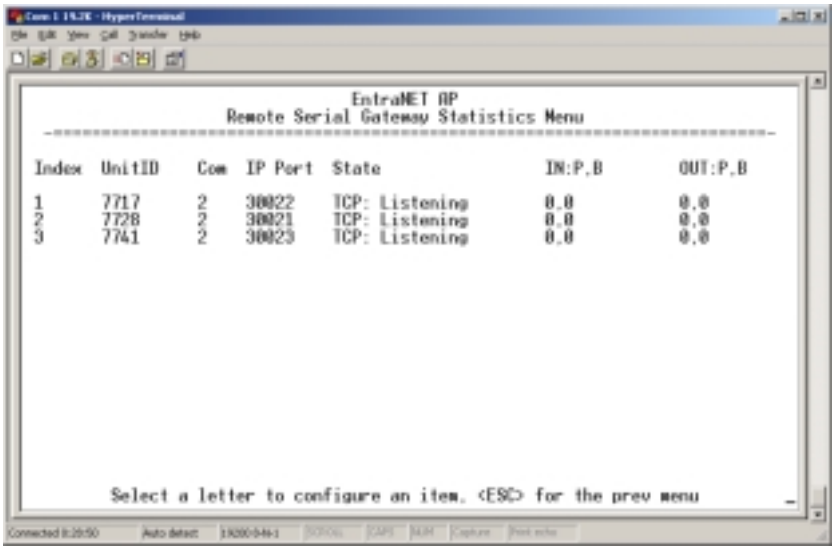


Figure 3-31. Serial Data Statistics Screen (Verify as latest screen)
(Both COM1 and COM2 are shown, as applicable)

- **`UnitID`**—The unit ID of the connected Remote.
- **`Com`**—Communication port being monitored (COM1 or COM2).
- **`IP Port`**—IP port associated with the listed device.
- **`State`**—State of the AP's server for this Remote. [Listening; Connected]

3.8.3 Ethernet and Wireless Packet Statistics Menus

The Ethernet/Wireless Packet Statistics Menu (Figure 3-32) shows vital data on packets and bytes sent/received, and errors detected. The screen is continuously updated at a refresh rate of approximately 3 seconds.

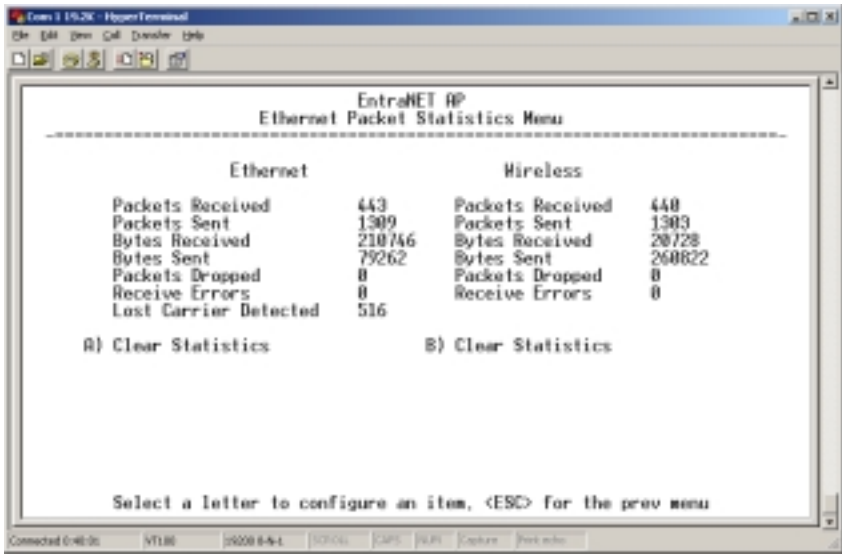


Figure 3-32. Sample Packet Statistics Menu (Ethernet shown)

Wireless Packet Statistics

- **Packets received**—Over-the-air data packets received by this unit
- **Packets sent**—Over-the-air data packets sent by this unit.
- **Bytes received**—Over-the-air data bytes received by this unit.
- **Bytes sent**—Over-the-air data bytes sent by this unit.
- **Packets dropped**—Received packets dropped as a result of a lack of buffers.
- **Receive errors**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.
- **Clear Wireless Statistics**—Resets the statistics counter.

Ethernet Packet Statistics

- **Packets received**—Packets received through the transceiver's Ethernet port.
- **Packets sent**—Packets received by the transceiver through the Ethernet port.
- **Bytes received**—Data bytes received by this unit.
- **Bytes sent**—Data bytes sent by this unit.
- **Packets dropped**—Received packets dropped as a result of a lack of buffers.
- **Receive errors**—Packets discarded after exceeding five retries the network.
- **Lost carrier detected**—A count of how many times the carrier signal on the Ethernet port has been missing. This count increase significantly when the Ethernet cable is inserted or removed.
- **Clear Ethernet stats**—Resets the statistics counter.

3.8.4 Radio Packet Statistics

The previous screen dealt with Ethernet-related information. The Radio Packet Statistics menu (Figure 3-33) contains statistics that relate directly to over-the-air transmission of data. It provides valuable insight into the quality of the RF link between entraNET units with respect to the handling of data packets.

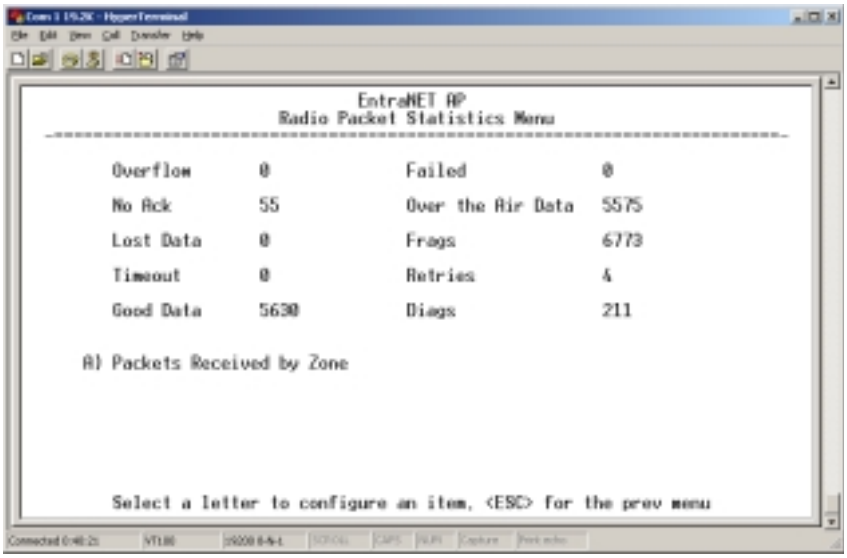


Figure 3-33. Radio Packet Statistics Menu

- **Overflow**—TX packets with “lcp buffer overflow” data responses.
- **No Ack**—Number of packets that were sent but not acknowledged.
- **Lost Data**—TX packets lost; over-the-air retries exceeded.
- **Timeout**—TX data packets lost; contention timeout.
- **Good Data**—Data packets with Cyclic Redundancy Check (CRC) “good” responses.
- **Failed**—TX packets failed; data integrity failed.
- **Over the Air Data**—Data packets successfully delivered over-the-air.
- **Frags**—Total fragments of data received.
- **Retries**—Total number of times packets were re-transmitted.
- **Diags**—TX packets with “Remote not Synchronized” data responses.

3.8.5 Event Log Menu

The transceiver’s microprocessor monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in Table 3-1. Some of these events will result from a condition that prevents the normal of the unit—these are “critical”

events. These will cause the unit to enter an “alarmed” state and the POWER LED to blink until the condition is corrected. All events are stored in the Events Log that can hold about 5000 entries**.**

Table 3-1. Event Classifications

Level	Description/Impact
Informational	Normal operating activities
Minor	Does not affect unit operation
Major	Degraded unit performance but still capable of operation
Critical	Prevents the unit from operating

Time and Date

The events stored in the Event Log are time-stamped using the time and date. The user must manually enter the date and time at the Access Point. (See *“DEVICE INFORMATION MENU”* on Page 64. The manually set time and date clock is backed up by an internal battery.

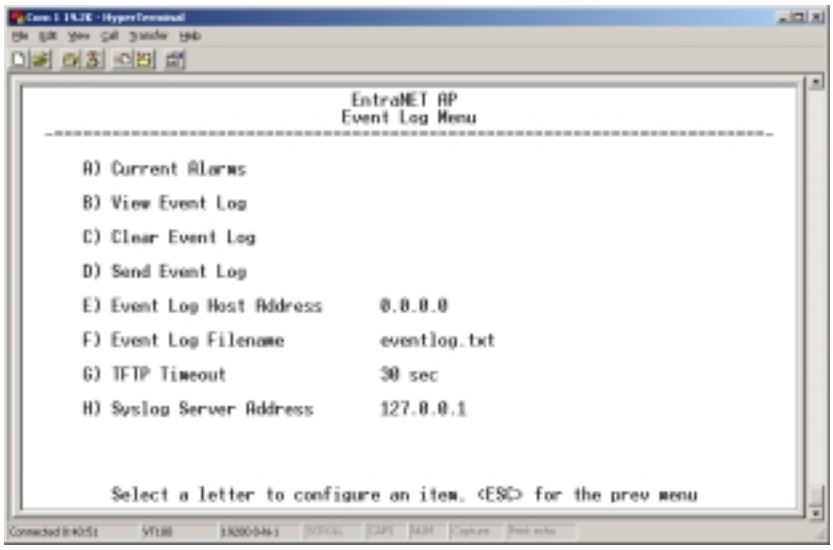


Figure 3-34. Event Log Menu

- **`Current Alarms`** *(Telnet/Terminal only)*—View list of root causes that have placed the Device Status in the alarmed state.
- **`View Event Log`** (see Figure 3-35)—View a list of events stored in the current log. Some of these events are stored in volatile memory and will be erased with a loss of power.

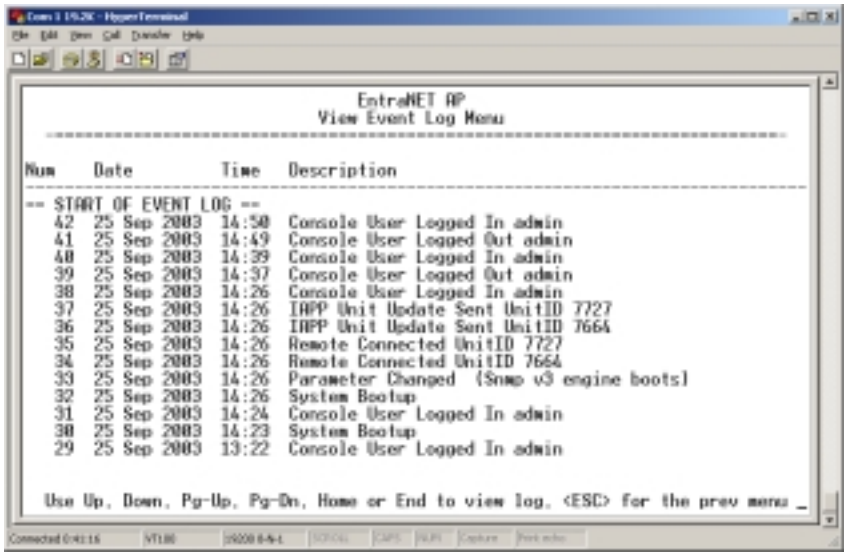


Figure 3-35. View Event Log Menu

- **`Clear Log`**—Purges the log of all stored events.

  TIP: Save your Event Log before choosing to clear it in order to retain potentially valuable troubleshooting information. (See *"Upgrading the AP'S Firmware"* on Page 67 for an overview on how to transfer files from the transceiver to a computer on the network using TFTP.)

- **`Send Event Log`** *(Telnet/Terminal only)*—Initiate TFTP transfer of the unit's event Event Log in a plain text (ASCII) file to a TFTP server on the connected LAN.
- **`Event Log Host Address`** *(Telnet/Terminal only)*—IP address of the computer on which the TFTP server resides. [Any valid IP address; 127.0.0.1]
- **`Event Log Filename`** *(Telnet/Terminal only)*—Name to be given to the Event Log file sent to the TFTP server for archiving.
  [Any 40-char alphanumeric string; Blank]

  NOTE: You may want to change it to reflect the type of log you intend to archive and/or its date.
- **`TFTP Time-out`** *(Telnet/Terminal only)*—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer.
  [10 to 120 seconds; 10]
- **`Syslog Server Address`**—The unit can also pass log messages on as they occur to a syslog server. Use this field to enter the IP address of this server.

3.9 DEVICE INFORMATION MENU

Figure 3-36 is the menu/screen that displays basic administrative data on the unit to which you are connected. It also provides a date and time display, Console Baud Rate setting, and user- specific parameters under the Device Names selection.

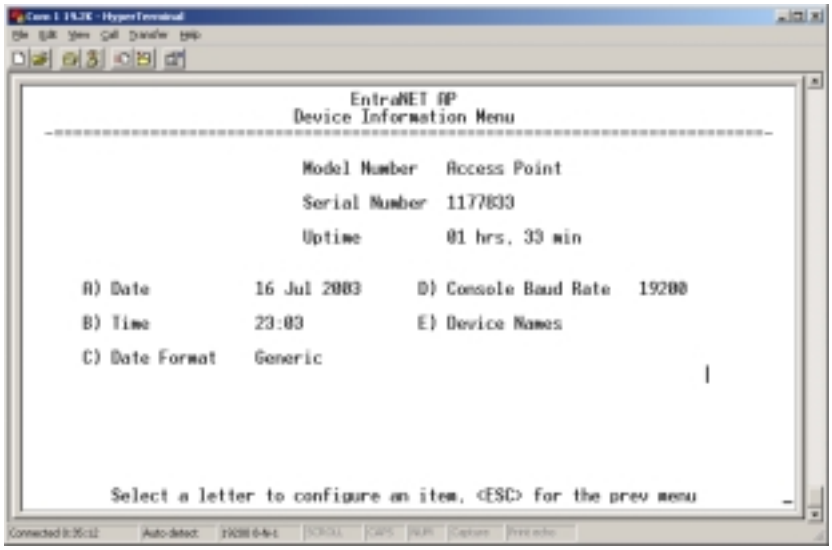


Figure 3-36. Device Information Menu

- **`Model Number`** *(Display only)*
- **`Serial Number`** *(Display only)*
- **`Uptime`** *(Display only)*—Elapsed time since powering up the unit.
- **`Date`**—Current date being used for the transceiver logs (user-settable). User-setable. Time of day is backed up by an internal battery.
- **`Time`**—Current time of day. User-setable.
  Setting: HH:MM:SS
  Time of day is backed up by an internal battery.
- **`Date Format`**—Select presentation format:
  - Generic = dd Mmm yyyy
  - European = dd-mm-yyyy
  - US = mm-dd-yyyy
- **`Console Baud Rate`**—Allows setting the console baud rate to match the connected terminal.
- **`Device Names Menu`** (Figure 3-37)—These fields are used at the user's discretion for administrative purposes. The Device Name field is used by the transceiver as the "Realm" name for network security and as the entraNET MS screen heading. All other entries appear on this screen only.

Device Names Menu

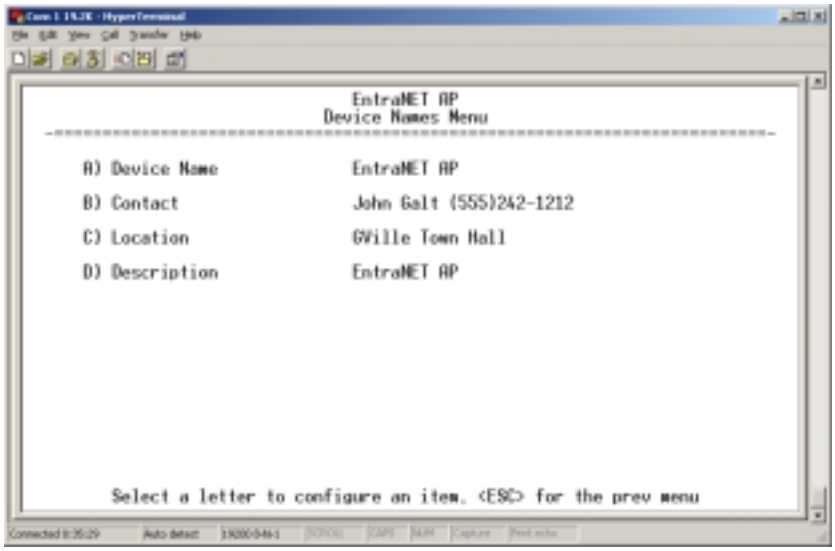


Figure 3-37. Device Names Menu

- **`Device Name`**—Device Name, used by the transceiver as the "Realm" name for network security and menu headings.
- **`Contact`**—User defined; appears on this screen only.
- **`Location`**—User defined; appears on this screen only.
- **`Description`**—User defined; appears on this screen only.

3.10 MAINTENANCE/TOOLS

In the normal course of operating your network, you will want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers. The *Maintenance Menu* provides several tools to make this possible. This section provides detailed information on how to use these services.

The three key maintenance tasks are:

- Reprogramming— Managing and selecting the unit's operating system firmware resources. *(See "Reprogramming Menu"* on Page 66*)*
- Configuration Scripts—Saving and importing data files containing unit operating parameters/settings. *(See " Configuration Scripts Menu"* on Page 70*)*
- Ping Utility—Diagnostic tool to test network connectivity. (See *" Ping Utility Menu"* on Page 77)
- Authorization Key —Alter the unit's overall capabilities by enabling the built-in resources. (*See "Authorization Keys Menu"* on Page 78*)*

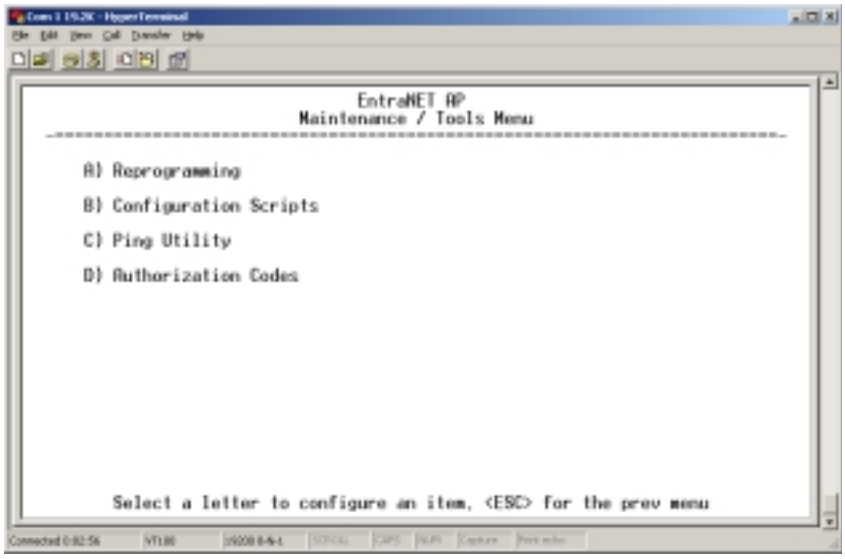


Figure 3-38. Maintenance/Tools Menu

3.10.1Reprogramming Menu

The AP transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is “active” and the second one is standing by, ready to be used. You can upload a new release into the inactive position and place it in service whenever you desire.

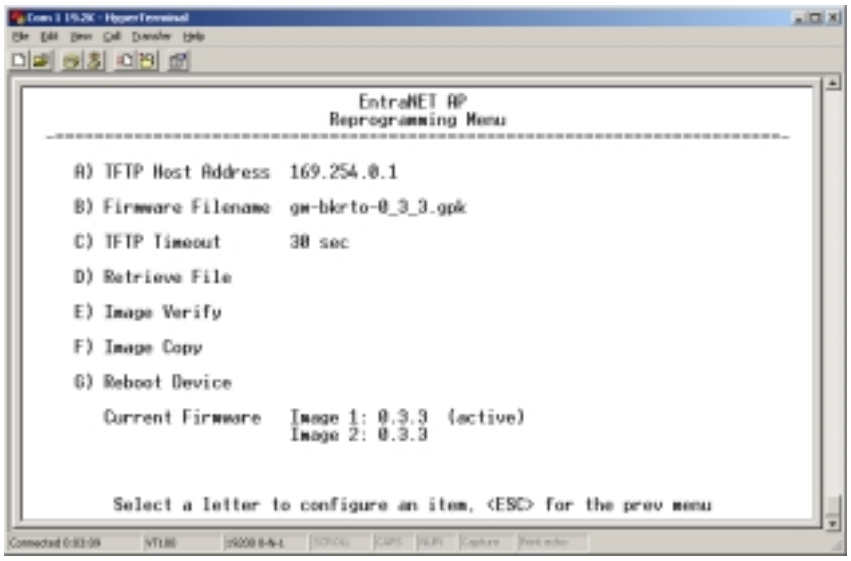


Figure 3-39. Reprogramming Menu
(Shown with “Image Copy” Selected)

- **`TFTP Host Address`**—IP address of the host computer from which to get the file. [Any valid IP address]

- **`Firmware Filename`**—Name of file to be received from the TFTP server.
  [Any 40-character alphanumeric string] Verify that this corresponds to the TFTP directory location. May require sub-directory, for example: **entranet/bkrfto-1_0_0.gpk.**
- **`TFTP Timeout`**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 seconds; 10]
- **`Retrieve File`**—Initiate the file transfer from the TFTP server. Placed into inactive firmware position in the transceiver's non-volatile memory [Y, N]
- **`Image Verify`**—Initiate the verification of the integrity of firmware file held in unit.
- **`Image Copy`**—Initiate the copying of the active firmware into the inactive image.
- **`Reboot Device`**—Initiate rebooting the transceiver. This will interrupt data traffic through this unit, and the network if performed on an Access Point. Intended to be used to toggle between firmware images.

  NOTE: See *"Upgrading the AP'S Firmware"* on Page 67 for details on setting up the TFTP server.
- **`Current Firmware`**—Shows the current firmware revision level.

Upgrading the AP's Firmware

From time-to-time MDS offers upgrades to the transceiver firmware. One version of the firmware provides core software resources for all radio models. Uploading new firmware into the unit will not alter any privileges provided by Authorization Keys and does not require the transceiver to be taken off-line until you want to operate the unit from the new firmware image in the unit.

You must use the entraNET Management System for all firmware activities, including uploading from a TFTP server.

NOTE: To upgrade the Remote firmware, refer to *UPGRADING REMOTE FIRMWARE*, on Page 93.

The uploads can be initiated through any of the three entraNET Management System gateways:

- **Terminal-Emulator**—Use a terminal emulator program on your PC, such as HyperTerminal, connected directly to the transceiver's COM1 port via a serial cable.
- **Telnet**—Text-based access to the Management System through a network connection.

- **Web Browser**—Connect to the transceiver using a Web browser on a local PC connected directly to the transceiver's LAN port or associated network.

Firmware images are provided free-of-charge on the MDS Web site at: **www.microwavedata.com/service/technical/support**

Upgrading the Transceiver Firmware

To install firmware by TFTP, the user will need:

- A PC with a TFTP server running. (A TFTP Server is available for download from the MDS website—see below.)
- The IP address of the PC running the TFTP server.

If you do not know your computer's IP address (Windows PC), you can use the **RUN** function from the **Start** menu and enter **winipcfg** or **ipconfig** to determine this information. The IP address of the radio can be found under the **Network Configuration** menu. (*See "Network Configuration Menu"* on Page 34.)

A TFTP server can be found on the MDS Web site at: **www.microwavedata.com/service/technical/support/downloads.asp**

There are several options for connecting the transceiver and computer control point to the firmware server. Figure 3-40 and Figure 3-41 show two variations.With either method, it is essential that all of the equipment be on the same subnet.

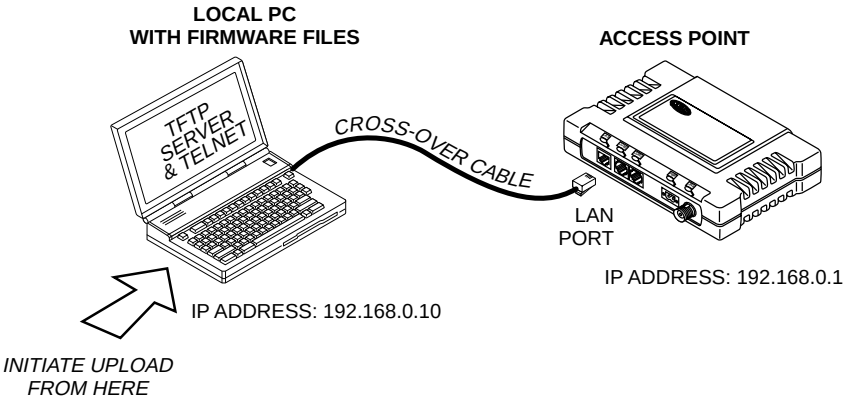


Figure 3-40. Upgrade Configuration—Option 1
(TFTP Server and Firmware File on Same CPU)

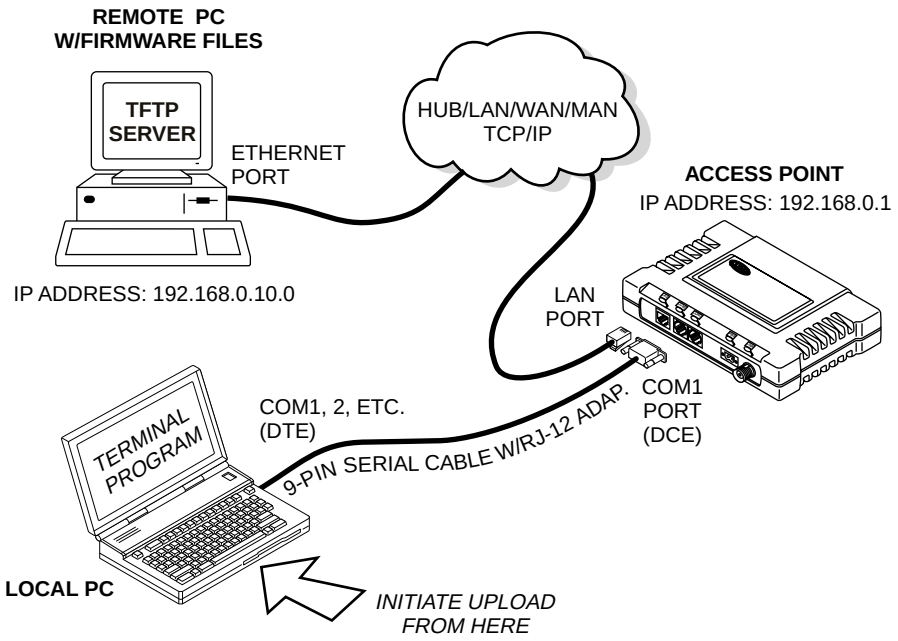


Figure 3-41. Upgrade Configuration—Option 2
(TFTP Server and Firmware File on Remote Server)

NOTE: Transferring the radio firmware image file (≈ 3 Mb), may take several minutes depending on traffic between the TFTP server and the transceiver.

Regardless of your connection to the transceiver, loading firmware/configuration files into the unit's flash-RAM is much slower than loading software onto a PC hard drive or RAM.

Upgrade Procedure

To upgrade the transceiver's firmware file (**filename.gpk**) use the following procedure:

1. Launch a TFTP server on a PC connected either directly or via a LAN to the Ethernet port (LAN) of the transceiver. Configure the server to allow downloads from the directory containing the firmware image file.

2. Connect to the entraNET Management System by whichever means is convenient: Browser or Telnet via the LAN, or Terminal emulator via the COM1 port.

3. Go to the entraNET MS Reprogramming Menu.
   (Main Menu>Maintenance Menu>Reprogramming Menu)

4. Fill in the information for the following:
   - **`TFTP Host Address`**—IP Address of server (host computer) running TFTP server.
   - **`Retrieve File`**—Name of file (**filename.gpk)** to be pulled from the TFTP server holding the firmware file.

5. Pull the firmware file through the TFTP server into the entraNET unit.
   (Main Menu>Maintenance Menu>Reprogramming Menu>Retrieve File)
   - Status messages on the transfer are posted on the PC screen. You can cancel the transfer at any time by pressing CTRL-C.
   - If the transfer does not start, verify that the AP and the PC can "ping" each other.

6. Reboot the transceiver to the new firmware image to make it active.
   Main Menu>Maintenance Menu>Reprogramming Menu>Reboot Device

7. Test the transceiver for normal operation.

End of Procedure

3.10.2 Configuration Scripts Menu

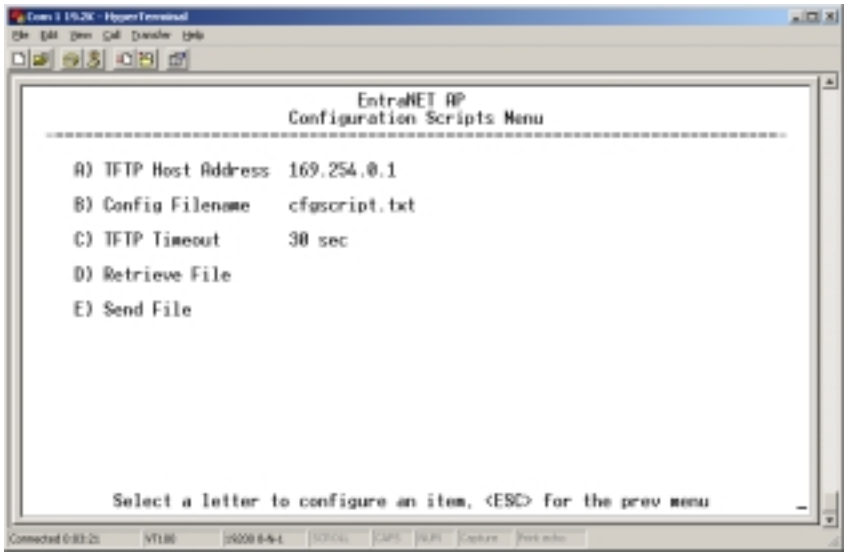


Figure 3-42. Configuration Files Menu

- **`TFTP Host Address`**—IP address of the computer on which the TFTP server resides. [Any valid IP address]
- **`Filename`**—Name of file containing this unit's configuration profile that will be transferred to the TFTP server. The configuration information will be in a plain-text ASCII format. [Any 40-character alphanumeric string] May require sub-directory, for example: **config\entranet-config.txt.** (See *"Using Configuration Scripts"* on Page 71)

  NOTE: The filename field is used in identifying the desired incoming file and as the name of file being exported to the TFTP server. Before exporting the unit's configuration, you may want to name it something that reflect the unit's services or identification.

- **`TFTP Timeout`**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 seconds; 10]
- **`Retrieve File`**—Initiate the file transfer of the configuration file from TFTP server into the transceiver.
- **`Send File`**—Initiate the file transfer from the transceiver's current configuration file to TFTP server.

NOTE: See *"Upgrading the AP'S Firmware"* on Page 67 for details on setting up the TFTP server.

A Brief Description of Configuration Files

If you plan to have more than a few transceivers in your network, use the Configuration Script feature to configure similar units from a common set of parameters. There are over 50 user-controllable settings that can be used to optimize the network and saved into a Configuration File. However, only four essential parameters need to be reviewed and altered to use the file with another transceiver.

A Configuration File (data file) will make it easy to apply your unique settings to any transceiver(s) you wish. Configuration files will also provide you with a tool to restore parameters to a "known good" set, in the event that a parameter is improperly set and performance is affected. (See *"Using Configuration Scripts"* on Page 71 for detailed instructions and a sample configuration file.)

Using Configuration Scripts

Configuration Scripts can be created and downloaded from the transceiver that contain a wealth of information on the unit. This file can serve many purposes, not the least of which is to keep a permanent "snapshot" of the unit's configuration at a point in time. These files can also be used to view the setup of a unit without needing to connect to it. Examining archival files can be a useful source of information during troubleshooting.

In the next few sections you will learn about the contents of the file and, how to use it as a template for configuring multiple transceivers with the same profile. Ultimately, standardized files can be uploaded into the transceiver to speed up the installation process.

Configuration Files can also be uploaded into a transceiver to restore the settings of a unit using a previously saved configuration of the unit. This is particularly convenient after finishing a test using some experimental settings.

Sample of an Exported Configuration File

The following is a sample of a typical configuration file as produced by a transceiver that contains over 150 parameters; many of which are user-editable. The presentation has been slightly altered to allow notes

to appear below associated parameter lines. Some of the values used in the calibration of the unit's built-in test equipment have been deleted to reduce space. This presentation is offered as a guide to the type of information contained in the file. See *"Editing Configuration Files"* on Page 76 for further information.

NOTE: The parameter names and the data values from the Exported Configuration File are shown in bolded text. Any description will be found below in an indented paragraph. Descriptions for parameters that are functionally identical to both COM1 & COM2 are not repeated.

Beginning of Configuration File:

; MDS entraNET

; Created 01-03-2003 6:59:41

IP Address: 192.168.1.1

The IPv4 address of this unit. This field is unnecessary if DHCP is enabled.

NOTE: Changing the IP value via the network will cause a loss of communication with other devices unaware of the new address.

IP Netmask: 255.255.255.0

The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled.

IP Gateway: 0.0.0.0

The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled.

Ethernet Address: 00:06:3D:00:00:5D

The physical Ethernet MAC (Media Access Controller) address of the device. This value is set by the factory and cannot be changed.

Model Number: 900

The model number of this unit. This value is set by the factory and cannot be changed.

Serial Number: 1026295

The serial number of this unit. This value is set by the factory and cannot be changed.

Unit Name: Library Admin Office

A name for this unit. It appears at the top of every menu screen.

Owner: Hilltop College MIS

The name of the owner of this unit.

Contact: John Galt X232

The contact person regarding this unit.

Description: Link to Campus Server

A brief general description of this unit.

Location: Hollister Bldg. RM450

The physical location of this unit.

Com2 Port Config: 8N1

Configuration of character size, type of parity, and number of stop bits to be used

Max Remotes Allowed: 50

The maximum number of Remotes allowed to connect to this Access Point.

Device Mode: Access Point

Configures the unit to act as a Remote or an Access Point. The Access Point option is not allowed unless the unit is specifically ordered as such, or an Authorization Key has been purchased to allow it.

Hop Time: 28

The amount of time the unit spends at any given frequency in its hopping pattern. This field is only changeable by an Access Point. Remotes read the Masters value upon association.

Network Address: 100

The ID of the network this unit belongs to. The unit will only communicate with devices having identical *Network Addresses*.

Date Format: Generic

Specifies the format of the date.

- Generic = dd Mmm yyyy
- European = dd-mm-yyyy
- US = mm-dd-yyyy

Console Baud: 19200

The baud rate of the serial menu console. Default value is 19200 bps.

Company Name: MDS

Version Name: 06-1234567

Product Name: entraNET

RF Output Power Setpoint: 30

The desired amount of RF output power, measured in dBm.

Active Boot Image: 0

Skipped Hop Zone1: Active

Skipped Hop Zone2: Skip

Skipped Hop Zone3: Active

Skipped Hop Zone4: Active

Skipped Hop Zone5: Active

Skipped Hop Zone6: Active

Skipped Hop Zone7: Active

Skipped Hop Zone8: Active

Skipped Hop Zone9: Active

Skipped Hop Zone10: Active

Firmware TFTP Host IP: 63.249.227.105

Address of the TFTP Host from which firmware images are downloaded

Firmware TFTP Filename: entraNET-bkrto-3_0_0.gpk

Eventlog TFTP Host IP: 192.168.1.3

Address of TFTP Host to which to send the event log

Eventlog TFTP Filename: eventlog.txt

Config Script TFTP Host IP: 192.168.1.33

Address of TFTP Host to which to send/receive configuration script

Config Script TFTP Filename: entraNET_config.txt

SNMP Read Community: public

Community string for read access using SNMPv1

SNMP Write Community: private

Community string for write access using SNMPv1

SNMP Trap Community: public

Community string sent with traps using SNMPv1

SNMP Trap Manager #1: 0.0.0.0

IP Address of a SNMP manager to which traps will be sent

SNMP Trap Manager #2: 0.0.0.0

SNMP Trap Manager #3: 0.0.0.0

SNMP Trap Manager #4: 0.0.0.0

Auth trap enable: disabled

Setting to enable SNMP authentication traps

Trap Version: v1 Traps

Selects which SNMP trap format

Package 1 Version: 1.1.0

Indicates the version of firmware in Image 1

Package 2 Version: 1.1.0

TFTP Timeout: 20

Com1 Serial Data Enable: disabled

Setting to enable COM1 data mode

Com1 Serial Data Mode: UDP

IP Protocol for COM1 data mode

Com1 Serial Data Baud Rate: 9600

Baud rate for COM1 data mode

Com1 Serial Data Tx IP Address: 0.0.0.0

COM1 data will be sent to this IP address

Com1 Serial Data Tx IP Port: 0

COM1 data will be sent to this IP port

Com1 Serial Data Rx IP Port: 0

COM1 data will be received on this IP port

Com2 Serial Data Enable: enabled

Com2 Serial Data Mode: UDP

Com2 Serial Data Baud Rate: 9600

Com2 Serial Data Tx IP Address: 169.254.10.2

Com2 Serial Data Tx IP Port: 0

Com2 Serial Data Rx IP Port: 0

Com1 Serial Data Rx IP Address: 0.0.0.0

COM1 data will be received on this IP address

Com2 Serial Data Rx IP Address: 169.254.0.2

Com2 Serial Data Flow Control: disabled

Setting to enable hardware flow control (RTS/CTS) in COM2 data mode

SNTP Server IP: 0.0.0.0

The IPv4 address of NTP/SNTP Time Server

Com1 Serial Data Seamless Mode: enabled

Setting to enable seamless mode for COM1 data mode

Com2 Serial Data Seamless Mode: enabled

Com1 Serial Data Delimiter Chars: 4

Minimum number of characters which will be considered a gap in seamless mode for COM1

Com2 Serial Data Delimiter Chars: 4

Com1 Serial Data Buffer Size: 20

Number of output characters which will be buffered in seamless mode for COM1

Com2 Serial Data Buffer Size: 20

RF Frequency Hopping Format: USA/CANADA

(Read Only) The frequency-hopping rules the radio is configured to operate under

SNMP Enable: disabled

Enable/Disable SNMP Agent

Approved Remotes List Enable: disabled

Setting to enable the Approved Remotes List

Encryption Enable: disabled

Setting to enable over-the-air data encryption

HTTP Enable: enabled

Setting to enable the HTTP interface

Telnet Enable: enabled

Setting to enable the Telnet interface

HTTP MD5 Authentication: disabled

Setting to enable MD5 Digest Authentication

End of Configuration File

Editing Configuration Files

Once a Remote unit's operation is fine-tuned, use the *Configuration Scripts Menu*, on Page 70 to save a copy of the configuration in a PC. When the file is saved in the PC it can be used as a source to generate modified copies adjusted to match other devices. The configuration files can be modified using a text editor or an automated process. (Not provided by MDS).

We recommend that you review and update the following parameters for each individual unit. Other parameters may also be changed.

Table 3-2. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio	Any legal IP address
IP Gateway	May change for different groups or locations	Any legal IP address
Unit Name	Should reflect a specific device. This information will appear in entraNET Management System headings	Any 20-character alphanumeric string
Location	Used only as reference for network administration	Any 40-character alphanumeric string
Radio Net(work) Address	Used to identify different groups or locations	1-20000

Each resulting file should be saved with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate its identification.

Editing Rules

- You may include only parameters you want to change.

- Change only the parameter values.
- Capitalization counts in some field parameters. (Example: System Mode)
- Comment Fields

    a. Edit, or delete anything on each line to the right of the comment delimiter, the semicolon (;).

    b. Comments can be of any length, but must be on the same line as the parameter, or on a new line that begins with a semicolon character.

    c. Comments after parameters included in files exported from a transceiver do not need to be present in your customized files.

3.10.3 Ping Utility Menu

The Ping Utility Menu (Figure 3-43) is used to verify IP connectivity with LAN nodes or Ethernet endpoints.

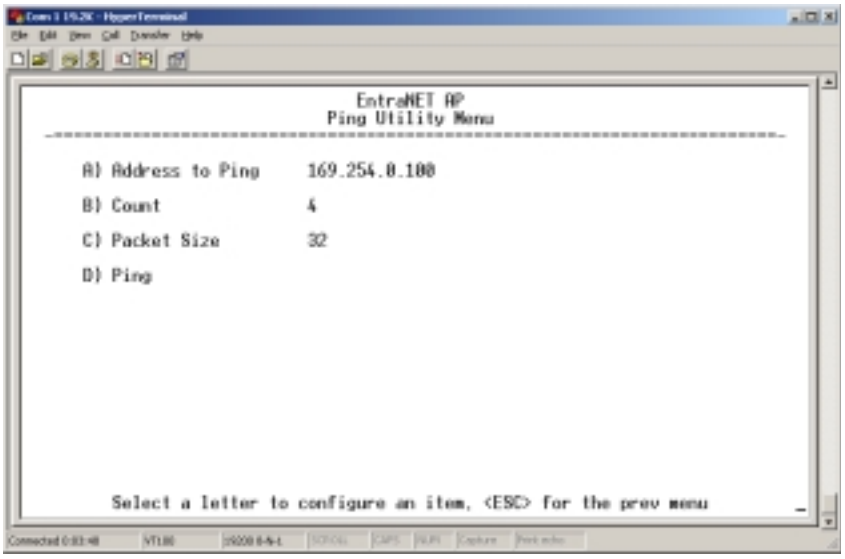


Figure 3-43. Ping Utility Menu

- **`Address to Ping`**—Address to send a PING. [Any valid IP address]
- **`Count`**—Number of PING packets to be sent.
- **`Packet Size`**—Size of each PING data packet (bytes).
- **`Ping`**—Start sending PING packets to address shown on screen. The process can be stopped at any time by pressing CTRL-C.

  Screen is replaced with a detailed report of PING activity. Press any key after viewing the results to return to this menu.

3.10.4Authorization Keys Menu

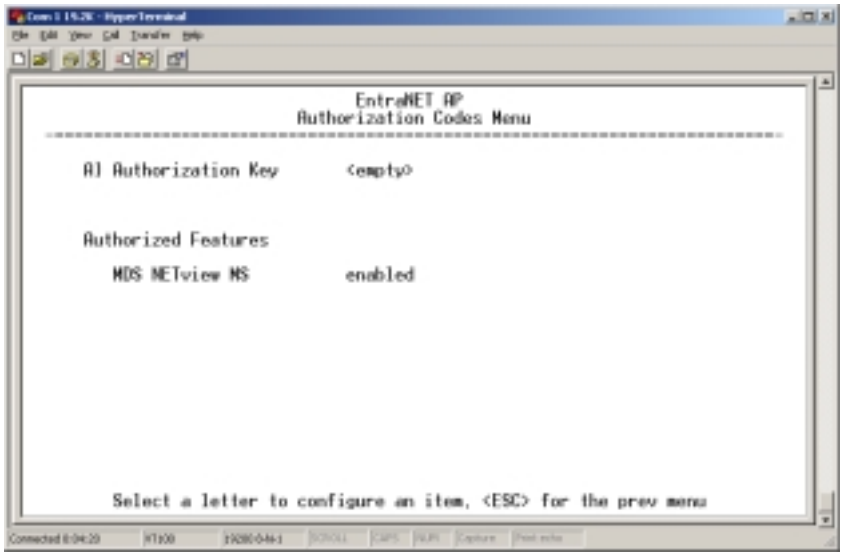
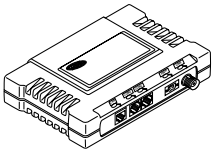


Figure 3-44. Authorization Keys Menu

- **`Authorization Key`**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **`Authorized Features`**—List of authorized features.

  In this example, *MDS NETview MS* is shown. This software product is intended to help users monitor system performance, configure network elements, detect faults and correct problems in the convenience of an office setting or at any other point in the network.



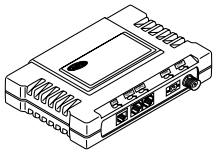
4 REMOTE RADIO MANAGEMENT

Contents

4.1 INTRODUCTION 81

4.1.1 Programming Methods 81
Terminal Interface Mode 81
Remote Management via the AP 81
PC-Based Configuration Software 81
4.1.2 User Commands 81
Entering Commands 81
Command Responses 82
4.1.3 Minimum Remote Configuration 82
4.1.4 Detailed Command Descriptions 83

4.2 UPGRADING REMOTE FIRMWARE 93



4.1 INTRODUCTION

The configuration of Remote transceivers is performed through a PC terminal connected to the radio's COM1 port. There are no manual adjustments or jumper settings required for configuration. This section explains how to establish a terminal session with the Remote and provides a complete list of user commands.

4.1.1 Programming Methods

Terminal Interface Mode

A PC program, such as HyperTerminal, may be used to provide a terminal session to enter the commands listed in Table 4-1 below. The PC must be connected to the radio via its COM1 connector.

When a PC terminal is used to connect to the radio, the settings of the program must match those of the radio. The default settings are: 19,200 bps, 8 data bits, no parity, 1 stop bit, and no handshaking.

You must log into the radio in order to issue commands. Only the **login** command is valid until this is done.

Log into the transceiver as follows:

At the **entranet>** prompt, type **login**
At prompt, enter username (Default=**admin**)
At prompt, enter Password (Default=**admin**)

Remote Management via the AP

Many Remote parameters may be configured over-the-air using the AP Management System. For more information on Remote Management via the AP, refer to *WIRELESS NETWORK MENU*, on Page 51.

PC-Based Configuration Software

Available soon—Contact MDS for information.

4.1.2 User Commands

Table 4-1 provides a quick-reference to the various user commands for the Remote transceiver. Detailed descriptions for these commands are presented in Section 4.1.4.

Entering Commands

The proper procedure for entering commands is to type the command, followed by an ENTER keystroke. For programming commands, the command is followed by SPACE, the appropriate information or values, and then ENTER. Use **COMMAND_ARG=** syntax to query a setting or value. Use **COMMAND_ARG=ARG=VALUE** syntax to set values.

Command Responses

The transceiver supports two command response formats—standard (plain language) and a hex format that may be copied into a configuration script. If you enter 0 after a command, the command executes normally (plain language). If you enter 1 after the command, the response is reported in hex format. Hex format is useful for automated processing of response data.

4.1.3 Minimum Remote Configuration

Remote radios require little configuration to operate, as most of the configuration is executed at the AP. The minimum set of parameters that need to be set at a Remote are as follows:

RADIO NETADDR—Radio's Network Address. Must match AP's address.

RADIO UNIT—32-bit unit address. Defaults to radio's serial number, but is user programmable.

RADIO PWR—RF output power setting. Value is in dB, with range of 20 (0.1 watt) to 30 (1 watt).

Table 4-1. Remote Commands—Quick Reference

COMMAND	DESCRIPTION
ALARM	Display current alarm conditions by class
APLIST	Set/display serial numbers of up to 10 APs with which the Remote should accept registration
AUTH	Set/display the authorization key and a list of authorized features
COM1	Set/display the configuration of COM1 port (baud rate, data format, buffer size, inter-packet gap)
COM2	Set/display the configuration of COM1 port (baud rate, data format, buffer size, inter-packet gap)
CONFIG	Shows the dump configuration of all settable parameters
DEVICE	Set/display device configuration. Here, items such as Owner, Company, and Serial Number may be found.
DIRECT	Set/display the configuration for direct mode operation
ENCRYPT	Set/display the configuration for data encryption
ETH	Set/display the configuration of the Ethernet port
HANDOFF	Set/display the configuration of hand-off capability
HELP	Lists commands supported for the level of the logged in user
LOG	Set/display the event log information
LOGIN	Secure login. Prompts user for case sensitive username and password
LOGOUT	Logs user off and ends terminal session
PASSWORD	Sets the user login password for user at current access level or less

Table 4-1. Remote Commands—Quick Reference *(Continued)*

COMMAND	DESCRIPTION
PROGRAM	Allows a boot to the bootloader
RADIO	Set/display the radio configuration and status
REBOOT	Restart the radio's firmware
SLEEP	Selects one of the low power operating modes: Sleep, Shutdown
STATS	Shows radio statistics
VER	Set/display the current version information

4.1.4 Detailed Command Descriptions

HELP

Lists commands supported for the current user login level.

ALARM
[<LEVEL>, HEX=]

This command displays the current alarm conditions by level. For each level, the specific events that caused the alarm are listed underneath along with brief descriptions. Alarm levels are:

ALL—All alarm classes
INFORM—Non-persistent information
MAJOR—Major alarm
CRITICAL—Critical alarm

Optional Arguments:

HEX= Read Only information. Displays the Alarm Hex Bits-Codes. It lists the hex bit codes for the current alarm condition by class. For each specific event that causes an alarm, the corresponding bit is set. Event numbers are matched to the appropriate hex code by a relationship of 2^n.

APLIST
[CLEAR, RESTRICT=<restrict>, APx=apx, CMD=<cmd>]

Sets/displays the serial numbers of up to ten APs with which the Remote should accept registration. A serial number of "0" indicates the slot is empty.

Optional Arguments:

CLEAR—Clears all entries in the AP list.

RESTRICT=<restrict>—Turns on/off restricting registration to access points. ON: Restricts registration to approved AP list, OFF: Does not restrict registration to approved AP list.

APx= —AP units, where x = 1 to 10. Sets / displays the serial number for one of 10 approved APs with which the Remote should accept connection. A serial number of 0 is used to delete an entry and indicates the slot is not filled.

AP1=<integer>Serial Number of approved AP
AP2=<integer>Serial Number of approved AP
AP3=<integer>Serial Number of approved AP
AP4=<integer>Serial Number of approved AP
AP5=<integer>Serial Number of approved AP
AP6=<integer>Serial Number of approved AP
AP7=<integer>Serial Number of approved AP
AP8=<integer>Serial Number of approved AP
AP9=<integer>Serial Number of approved AP
AP10=<integer>Serial Number of approved AP

AUTH

[KEY=<key>, CMD=<cmd>]

This command is used to set / display the authorization key and a list of authorized features.

Optional Arguments:

KEY=<key>—Add (or display last) authorization key, which is used to enable / disable software features. Length: 1-16 characters.

COM1

[DEFAULT=<default>, MODE=<mode>, BAUD=<baud>, FORMAT=<format>, BUFFER=<buffer>, DELAYCHARS=<chars>]

Sets / displays configuration of COM1 port.

Optional Arguments:

DEFAULT=<default>—Sets / displays default mode of COM1 port on bootup. COM1 DEFAULT cannot be set to DATA unless the device has been authorized for serial payload.

CONSOLE: COM1 defaults to Command-line mode.
DATA: COM1 defaults to transparent data mode

MODE=<mode>—This immediately switches the console port among various interface modes. Cannot be set to DATA unless the device has been authorized for serial payload. To escape from data mode, enter three consecutive '+' characters to COM1 with at least 100 mSec between entries.

CONSOLE: COM1 in Command-line mode
DATA: Com1 in transparent data mode

BAUD=<baud>—Sets / displays baud rate setting as1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 230400 bps

FORMAT=<format>—Sets / displays data characters, parity, and stop bits setting of the COM port. Valid data parameters are:

7N1—7 char bits, no parity, 1 stop bit
7N2—7 char bits, no parity, 2 stop bits
7O1—7 char bits, odd parity, 1 stop bit
7O2— 7 char bits, odd parity, 2 stop bits
7E1—7 char bits, even parity, 1 stop bit
7E2—7 char bits, even parity, 2 stop bits
8N1—8 char bits, no parity, 1 stop bit (Default)
8N2—8 char bits, no parity, 2 stop bits
8O1—8 char bits, odd parity, 1 stop bit
8O2—8 char bits, odd parity, 2 stop bits
8E1—8 char bits, even parity, 1 stop bit
8E2—8 char bits, even parity, 2 stop bits

NOTE: Entry of data formats other than those listed above may cause undesired operation.

BUFFER=<buffer>—Sets / displays maximum buffer size of the COM port. Acceptable value range is 1–1500.

DELAYCHARS=<delaychars>—Sets / displays minimum inter-packet gap for the COM port. Acceptable value range is 1–256

COM2

[MODE=<mode>, BAUD=<baud>, FORMAT=<format>, BUFFER=<buffer>, DELAY-CHARS=<delaychars>]

This command Sets / displays the configuration of the COM2 port.

Optional Arguments:

MODE=<mode>—Sets / displays mode of the COM2 port. COM2 MODE cannot be set to DATA unless the device has been authorized for serial payload data.

DISABLED—COM2 data mode disabled
DATA—COM2 in transparent data mode

BAUD=<baud>—Sets / displays baud rate setting as1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 230400 bps.

Sets / displays data characters, parity, and stop bits setting of the COM port. Valid data parameters are:

7N1—7 char bits, no parity, 1 stop bit
7N2—7 char bits, no parity, 2 stop bits
7O1—7 char bits, odd parity, 1 stop bit
7O2— 7 char bits, odd parity, 2 stop bits
7E1—7 char bits, even parity, 1 stop bit

7E2—7 char bits, even parity, 2 stop bits
8N1—8 char bits, no parity, 1 stop bit (Default)
8N2—8 char bits, no parity, 2 stop bits
8O1—8 char bits, odd parity, 1 stop bit
8O2—8 char bits, odd parity, 2 stop bits
8E1—8 char bits, even parity, 1 stop bit
8E2—8 char bits, even parity, 2 stop bits

NOTE: Entry of data formats other than those listed above may cause undesired operation.

BUFFER=<buffer>—Sets / display maximum buffer size of the COM port. Acceptable value range is 1–1500.

DELAYCHARS=<delaychars>—Sets / displays minimum inter-packet gap for the COM port. Acceptable value range is 1–256.

CONFIG
[SHOW, SAVE=]

Saves/Displays the current configuration. The output is in a format that may be copied back into the command line in order to set the configuration.

Optional Arguments:

SHOW—Displays the current configuration. This is a read-only response.

SAVE=—Saves the current configuration.

DEVICE
[COMPANY=, MODEL=, PROD=, SREV=, OWNER=<owner>, UPTIME=, SER=, XSNUM=, CMD=<cmd>]

This command sets / displays the device configuration. Items such as Owner, Company, and Serial Number can be found here.

Optional Arguments:

COMPANY= —Read Only. Sets / displays company name. Allowable length is 1–20 characters.

MODEL=— Read Only. Sets / displays unit model number. Allowable length is 1–20 characters.

PROD= —Read Only. Sets / displays product name. Allowable length: is 1–20 characters.

SREV= —Read Only. Sets / displays software revision ID. Allowable length is 1–15 characters.

OWNER=<owner>—Sets/displays owner information string. Owner can program any information (as one continuous string). Allowable length is 1–30 characters.

UPTIME= —Read Only. Displays current system uptime <YY-MM-DD hh:mm:ss>. Allowable length is 1–11 characters.

SER=— Read Only. Sets / displays device serial number. Acceptable value range is 1–99999999

XSNUM= —Read Only. Sets / displays Radio Board Serial Number. Acceptable value range is 0–99999999.

DIRECT

[DEFAULT=<default>, MODE=<mode>, STATE=, TYPE=<type>, NETADDR=<netaddr>, CMD=<cmd>]

Sets / displays the configuration for direct mode operation (Remote to Remote).

Optional Arguments:

DEFAULT=<default>—Sets / displays default DIRECT mode.

OFF: Direct Mode defaults to disabled
ON: Direct Mode defaults to enabled
EXT: Direct Mode defaults to control via external signal

MODE=<mode>—Sets / displays DIRECT mode setting

OFF: Direct Mode disabled
ON: Direct Mode enabled
EXT: Direct Mode controlled via external signal

STATE=— Read Only. Display status of DIRECT mode setting.

OFF: Direct mode state: off
ON: Direct mode state: on

TYPE=<type> Read / Write. Sets / displays whether device acts as root or node when in direct mode.

NODE: Direct type is Node

ROOT: Direct type is Root

NETADDR=<netaddr>—Sets / display Network (system) address when in direct mode. Acceptable value range is 0–32637.

CMD=<cmd>—If set to 0, the command executes normally. If <cmd> is set to 1, the command reports all settings in a format that may be copied into a configuration script.

ENCRYPT
[MODE=<mode>, PHRASE=<phrase>, CMD=<cmd>]

This command sets / displays the configuration for data encryption.

Optional Arguments:

MODE=<mode>—Sets / display data encryption mode

OFF: Data encryption off
ON: Data encryption on

PHRASE=<phrase>—Encryption Pass Phrase. Allowable length is 1–40 characters.

ETH
[MODE=<mode>, MACADDR=<macaddr>, CMD=<cmd>]

This commands set / displays the configuration of the Ethernet port.

Optional Arguments:

MODE=<mode>—Determines whether the Ethernet port is enabled or disabled.

OFF: Ethernet Port Disabled
ON: Ethernet Port Enabled

MACADDR=<macaddr>—Sets/ display Ethernet MAC address. Ethernet address should be in the following form: xx:xx:xx:xx:xx:xx

HANDOFF
[MODE=<mode>, BLOCKTIME=<blocktime>, AVGINT=<avgint>, MISSCOUNT=<misscount>, MISSPERCENT=<misspercent>, CMD=<cmd>]

This command sets / displays the configuration of hand-off capability.

Optional Arguments:

MODE=<mode>—Enable/disable hand-offs.

OFF: Hand-off is turned deactivated
ON: Handoff is activated

BLOCKTIME=<blocktime>—Time in seconds to block access to an Access Point after handoff.

AVGINT=<avgint>—Handoff averaging interval. *Available soon.*

MISSCOUNT=<misscount>—Number of missed ack packets before handoff. *Available soon.*

MISSPERCENT=<misspercent>—Handoff Threshold: Percentage of missed ack's before handoff. *Available soon.*

HELP

Lists commands supported for the current user login level.

LOG
[CLEAR, SHOW, TOTAL=, CMD=<cmd>]

This command sets / displays the event log information. Displays the number of entries in the event log. Optional arguments are used to clear or display the log.

Optional Arguments:

CLEAR—Clear the event log
SHOW—Show the event log
TOTAL= —Number of event log entries in log. Read only.

LOGIN

This command is used for secure login to the radio. At prompt, enter case sensitive username and password. Each of these entries can be up to 8 characters long.

LOGOUT

Used for logging out of the command interface.

PASSWORD
[<username>]

This command sets the user login password for user at current access level or below.

Optional Arguments:

<username>—The login username to be associated with the password.

PROGRAM
[VERIFY=<verify>]

This command allows a boot to the bootloader. At prompt, enter 'y' or 'n'.

Optional Arguments:

VERIFY=<verify>—Selects one or all images to perform checksum verification

ALL: All images
BOOT: Bootloader Image
APP1: App 1 Image
APP2: App 2 Image
TOR1: Tor 1 Image
TOR2: Tor 2 Image

RADIO

[UNIT=<unit>, NETADDR=<netaddr>, PWR=<pwr>, SYNC=, RSSI=, CONN=<conn>, AP=, REFRESH=<refresh>, CMD=<cmd>]

This command sets / displays the radio configuration and status.

Optional Arguments:

UNIT=<unit>—32-bit user-programmable unit address. Defaults to serial number but is user programmable.

NETADDR=<netaddr>—Current Radio Network Address. Acceptable value range is 0–32637

PWR=<pwr>—Current Radio Power Setting. Value is in dBm with an acceptable range of 20–30.

SYNC= Read only. Shows current state of radio synchronization.

RSSI= Read only. Shows Received Signal Strength (RSSI). Value is shown in dBm with a range of -120 to 0. This value is refreshed every three seconds.

CONN=<conn>—Determines whether the device (Remote) has associated with an Access Point.

NOT ASSOCIATED: Remote radio not associated with an AP
ASSOCIATED: Remote radio associated with an AP

AP= Read only. Shows associated AP's Serial Number. Acceptable value range is 1–99999999

REFRESH=<refresh>—Read only. Connection refresh period in seconds with an acceptable value range of 0–255

REBOOT

[REBOOT, SAME, OTHER, APP1, APP2]

This command is used to reboot the radio's firmware.

Optional Arguments:

SAME—Same Image
OTHER—Other Image
APP1—Application Image 1
APP2—Application Image 2

SLEEP

[SLEEP, MODE=<mode>, WAKE=<wake>, DTRSENSE=<dtrsense>, PERIOD=<period>, HANGTIME=<hangtime>, CMD=<cmd>]

This command sets/displays one of the low power operating modes the Remote radio will operate under. These modes are commonly used in

cases where power consumption must be kept to a minimum, such as in solar-powered installations.

Optional Arguments:

MODE=<mode>—Set mode as follows:

NONE: Normal

SLEEP: Sleep enabled. In this mode, the radio draws less than 20 mA at 12 volts. It can be brought back online (ready to send data) within 75 milliseconds. Wake-up is accomplished by asserting the DTR line on the COM2 port, or by the appearance of payload data at the active COM port.

SHUTDOWN: Shutdown enabled. Radio draws less than 1 mA @ 12 volts. This mode requires a longer wakeup time—almost as long as if the radio were de-powered.

WAKE=<wake>—This selects a control option to activate(enter) or deactivate(exit) sleep or shutdown modes.

DTR: Wake under DTR signal control
DATA: Wake up on data
PERIOD: Wake up periodically

DTRSENSE=<dtrsense>—DTR sense setting.

LOW: DTR Active LOW
HIGH: DTR Active HIGH

PERIOD=<period>—Wake-up period in seconds when SLEEP WAKE is set to PERIOD. Acceptable value range is 5–86400

HANGTIME=<hangtime>—Minimum wake time in seconds before returning to low power mode. Acceptable value range is 5–600

STATS

[ALL, RADIO, COM1, COM2, ETH, RESET]

This command displays radio statistics. If **<device>** (**RADIO,COM1,COM2,ETH**) is omitted, *all* statistics are displayed.

Optional Arguments:

ALL: Displays all statistics
RADIO: Displays radio packet statistics
COM1: Displays COM1 packet statistics
COM2:Displays COM2 packet statistics
ETH: Displays Ethernet packet statistics
RESET: Resets packet statistics for the indicated interface

VER

[VER, SWID1=, SREV1=, XSREV1=, SWID2=, SREV2=, XSREV2=, IMAGE=<image>, RADIOSW=, H2H=, CONFIG=, EVENT=, LOG=, HREV=, XHREV=, CMD=<cmd>]

This command sets/displays the current Version information for the radio.

Optional Arguments:

SWID1=—Shows current Software ID text (06-nnnnAnn). Allowable length is 1–10 characters.

SREV1=—Shows software version number (xx.yy.zz). Allowable length is 1–8 characters.

XSREV1= —Displays radio software version. Allowable length is 1–8 characters.

SWID2= —Shows current Software ID text (06-nnnnAn). Allowable length is 1–10 characters.

SREV2=—Shows software version number (xx.yy.zz). Allowable length is 1–8 characters.

XSREV2= —Displays radio software version. Allowable length is 1–8 characters.

IMAGE=<image>—Selects boot image index.

RESET: Go to Reset Vector
APP1: Application Image 1
APP2: Application Image 2

RADIOSW= —Shows current Radio Software Version number (xx.yy.zz). Allowable length is 1–15 characters.

H2H= — Host-to-Host protocol version number.

CONFIG= —Configuration Table version

EVENT= —This command is used to determine whether the current Event list properties need to be upgraded or not.

LOG= —This command is used to determine whether the current Log format needs to be upgraded or not.

HREV= —Displays OIB Board Hardware Revision. Allowable length: is 1–8 characters.

XHREV= —Radio Board Hardware Revision. Allowable length is 1–8 characters.

4.2 UPGRADING REMOTE FIRMWARE

A Remote radio's firmware may be upgraded using the Windows-based utility, *entraNET Remote Upgrade* software (Figure 4-1). A local PC connection to the radio is required for this upgrade. Follow the prompts and dialog boxes on the screen to perform the upgrade procedure. A description of these items appears below.

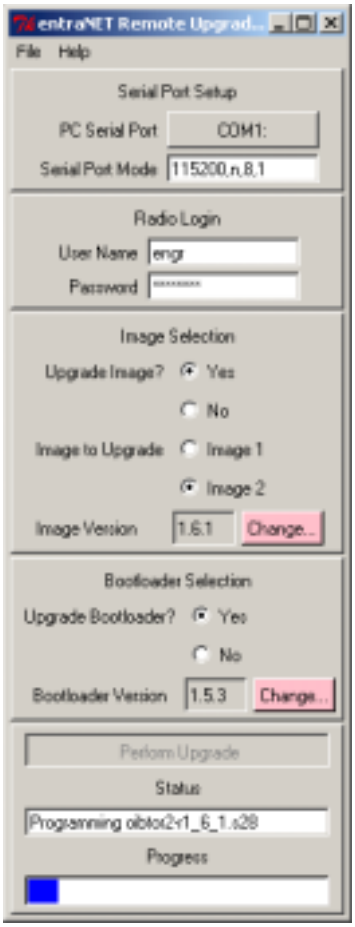
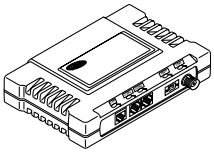


Figure 4-1. Remote Upgrade

- **`PC Serial Port`**—Set to the serial port on the PC to which the Remote is connected.
- **`Serial Port Mode`**—Enter the data rate, parity, data bits, and stop bits to use when connecting to the Remote's console (COM1) port.
- **`Image to Upgrade`**—Select the image of firmware you wish to upgrade.
- **`Image Version Change`**—Click this button to set the firmware version to upgrade to.
- **`Upgrade Bootloader`**—Select **Yes** to also upgrade the Remote's bootloader.
- **`Bootloader Version Change`**—Click this button to select the bootloader version to upgrade to.

- **Perform Upgrade**—Click this button to begin the upgrade process.
- **Status**—Shows the action being performed by the upgrade utility.
- **Progress**—Displays the progress of the current action.

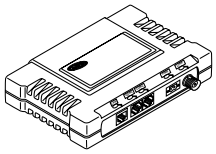


5 SAMPLE CONFIGURATIONS

Contents

5.1 INTRODUCTION 97

5.1.1 IP-to-Local Serial Application Example 97
5.1.2 IP-to-Remote Serial Application Example 98
5.1.3 Point-to-Point, Serial-to-Serial Application Example 99
5.1.4 Point-to-Multipoint Serial-to-Serial Application Example 100
5.1.5 Mixed Mode Application Example 101
Operation and Data Flow 101



5.1 INTRODUCTION

This chapter provides details of how radios should be configured and connected for specific applications, such as IP-to-Serial and Serial-to-Serial configurations. Only the most relevant parameters are shown for the sake of simplicity. All other parameters are assumed to be set at their default values.

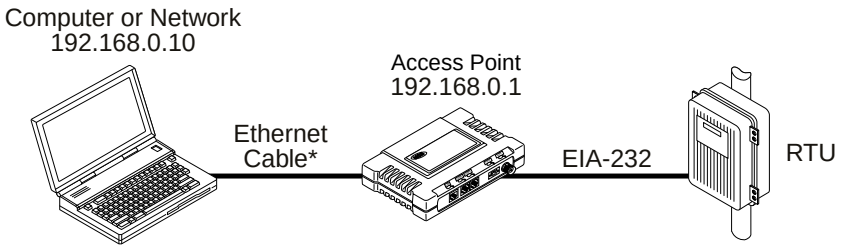
5.1.1 IP-to-Local Serial Application Example

You may use either UDP or TCP to establish communications with the entraNET. The choice will depend on the type of device you are communicating with at the other end of the IP network. In this example we will use TCP to illustrate this function.

In TCP mode, the transceiver remains in a passive state offering a socket for connection. When a request is received, data received by the AP's serial port will be sent out through the IP socket and vice versa, until the connection is closed, or the link is interrupted. The TCP session has a timeout of 10 minutes. If inactive for that time, it will be closed. The transceiver will offer again the port for connection after this time. (See Figure 5-1 and Table 5-1)

Establishing a Connection

From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured earlier (typically 30011). A Telnet client application can be used to establish this connection. Data can now be sent between the PC and the RTU or other connected device.



*Use crossover cable for computer; Straight-through cable for Network

Figure 5-1. IP-to-Local Serial Application Diagram

Table 5-1. IP-to-Local Serial Port Application Configuration
IP-to-Local Serial Connection (Local Serial Gateway)

Unit Location	Menu Item	Setting
Access Point (COM2)	Port Status	Enabled
	Mode	TCP
	RX IP Port	30011
	Baud Rate	19200
	Byte Format	8N1
	Seamless Mode	Disabled
	Buffer Size	256 Bytes
	Inter-Packet Delay	4

Table 5-2. IP-to-Local Serial Port Application Configuration
IP-to-Local Serial Connection (Local Serial Gateway)

Unit Location	Menu Item	Setting
Access Point (COM2)	Port Status	Enabled
	Mode	TCP
	RX IP Port	30011
	Baud Rate	19200
	Byte Format	8N1
	Seamless Mode	Disabled
	Buffer Size	256 Bytes
	Inter-Packet Delay	4

5.1.2 IP-to-Remote Serial Application Example

This configuration makes any data sent or received with the AP via an IP port number appear via the serial port of a single Remote (or of all Remotes if “Broadcast” is selected for Remote ID.

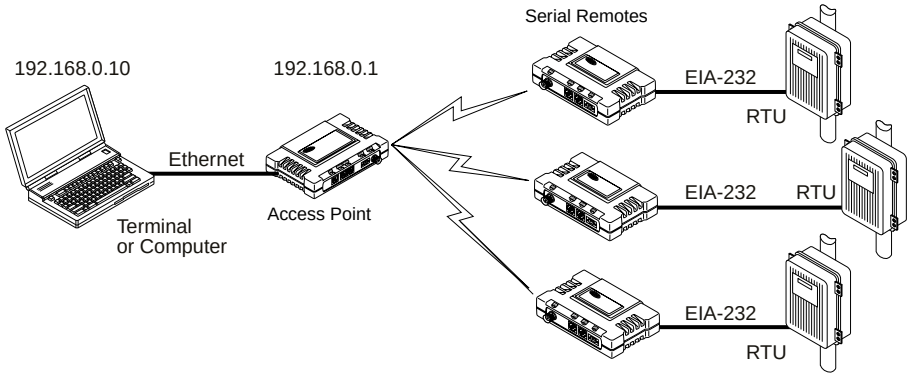


Figure 5-2. IP-to-Remote Serial Application Diagram

Table 5-3. IP-to-Remote Serial Application Configuration.

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)	Remote ID	1155883
	COM Port	COM2
	Mode	TCP Server
	Radio IP Port	30066
Remote Unit (COM2)	Mode	COM2 in transparent data mode
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4
	Seamless	TX data only

5.1.3 Point-to-Point, Serial-to-Serial Application Example

Once the transceivers are configured and the changes have been executed, they begin processing any data presented at the COM ports. Data presented at the Access Point's COM port is packetized and sent over the air via a proprietary protocol to the Remote. Upon receiving the packet, the Remote sends the data out its COM port. Likewise, data presented at the Remote's COM port is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port. Note that this configuration does *not* use multicast addressing.

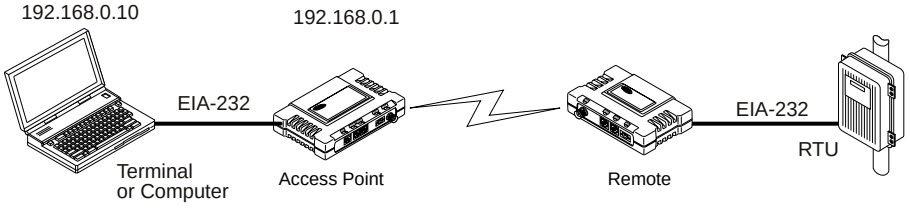


Figure 5-3. Point-to-Point Serial-to-Serial Application Diagram

Table 5-4. Point-to-Point Serial-to-Serial Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	1155999 (example)
	Rem. COM Port	COM2
	Baud Rate	19200
	Byte Format	8N1

Table 5-4. Point-to-Point Serial-to-Serial Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
	Seamless Mode	Disabled
	Buffer Size	256 Bytes
	Inter-Packet Delay	4
Remote Unit (COM2)	Mode	Data
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4

5.1.4 Point-to-Multipoint Serial-to-Serial Application Example

The operation and data flow for this mode is very similar to a Point-to-Point serial-to-serial application, except that it uses multicast addressing. The primary difference is that data presented at the Access Point's COM port will be packetized and sent to all of the Remotes. Upon receiving the packet all of the Remotes strip the data out of the packet and send it out their COM port. Likewise, data presented at any of the Remotes' COM ports is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port.

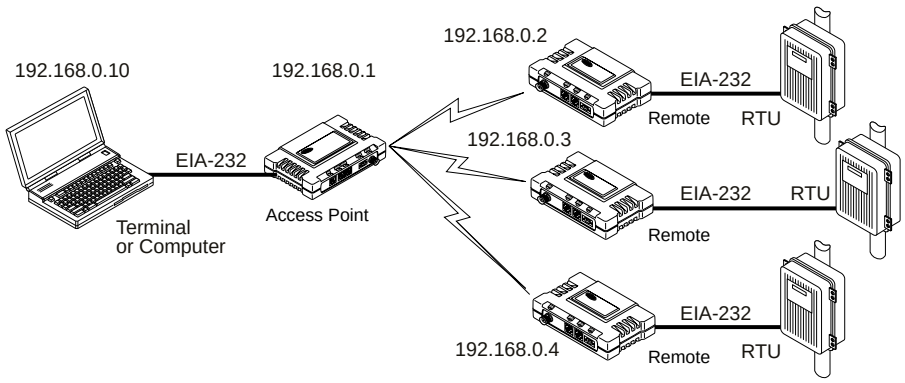


Figure 5-4. Point-to-Multipoint Serial-to-Serial Diagram

Table 5-5. Point-to-Multipoint Serial-to-Serial Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	Broadcast
	Remote COM port	COM2
	Baud Rate	19200

Table 5-5. Point-to-Multipoint Serial-to-Serial Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
	Byte Format	8N1
	Seamless Mode	Disabled
	Buffer Size	256 Bytes
	Inter-Packet Delay	4
Remote Unit (COM2)	Mode	Data
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4

5.1.5 Mixed Mode Application Example

In this configuration, the Host PC can use both TCP and Serial-to-Serial data paths to reach the RTUs. This may be helpful when a mixed collection of RTUs is present where some RTUs operate via Ethernet while others are polled via a serial port. (See Figure 5-5 on Page 101 and Table 5-6 on Page 102)

Operation and Data Flow

- Communicate with RTUs A and B by sending and receiving data from the AP's COM2 port.
- Communicate with RTUs C and D by Telneting to the IP address of each RTU.
- All communication paths can be used simultaneously.

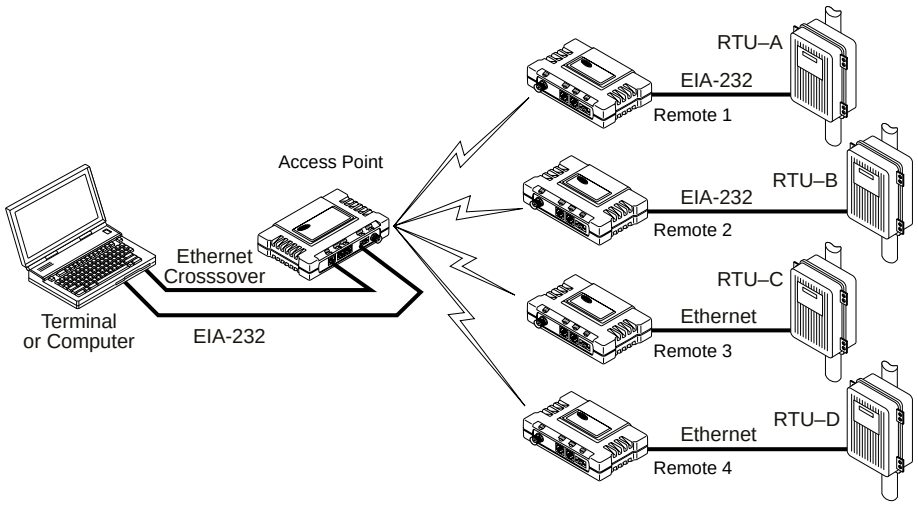
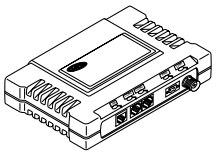


Figure 5-5. Mixed-Modes Application Diagram

Table 5-6. Serial Port Application Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	Broadcast
	Remote COM Port	COM2
	Baud Rate	19200
	Byte Format	8N1
	Seamless Mode	Disabled
	Buffer size	256 Bytes
	Inter-Packet Delay	4 Characters
Remote Units 1 & 2 (COM2)	Mode	Data
	Baud Rate	19200
	Data Format	8N1
	Buffer Size	256
	DelayChars	4
Remote Units 3 & 4 (ETH)	Mode	On



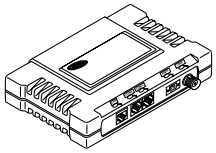
6 INSTALLATION

Contents

6.1 INSTALLATION 105

6.1.1 General Requirements 105
6.1.2 Site Selection 106
6.1.3 Terrain and Signal Strength 106
6.1.4 Antenna & Feedline Selection 107
6.1.5 Conducting a Site Survey 109
6.1.6 A Word About Radio Interference 109
6.1.7 How Much Output Power Can be Used? 111

6.2 dBm-WATTS-VOLTS CONVERSION CHART 113



6.1 INSTALLATION

This section provides tips for selecting an appropriate site, choosing an antenna system, and reducing the chance of harmful interference.

6.1.1 General Requirements

There are three main requirements for installing transceiver—adequate and stable primary power, a good antenna system, and the correct interface between the transceiver and the data device. Figure 6-1 shows a typical Remote installation.

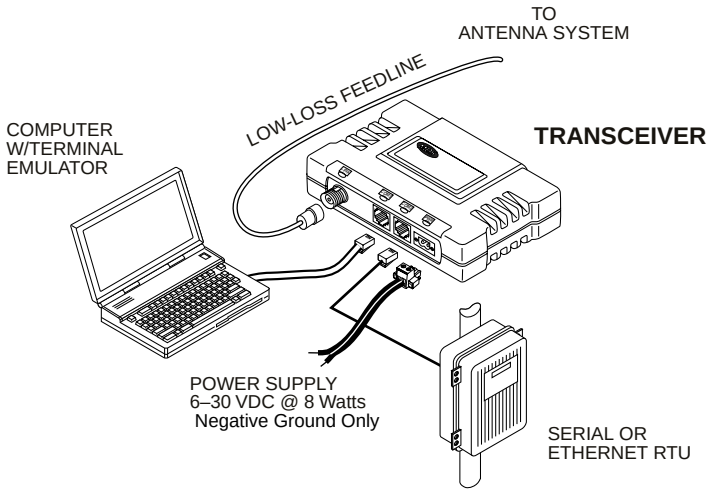


Figure 6-1. Typical Transceiver Installation (Remote Shown)

Mounting Dimensions

Figure 6-2 shows the dimensions of the AP transceiver with mounting brackets attached. Figure x shows the same view for a Remote transceiver.When mounting entraNET transceivers, choose a location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.

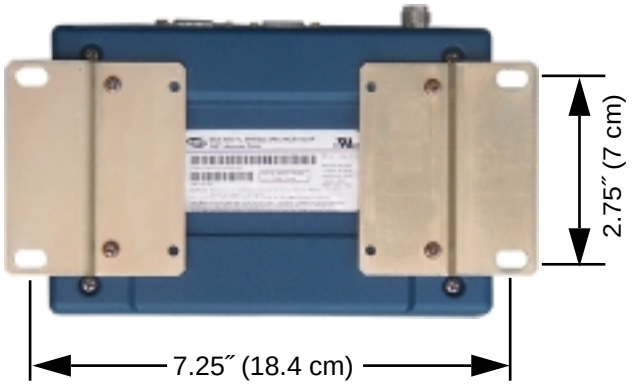


Figure 6-2. Mounting Bracket Spacing—Access Point

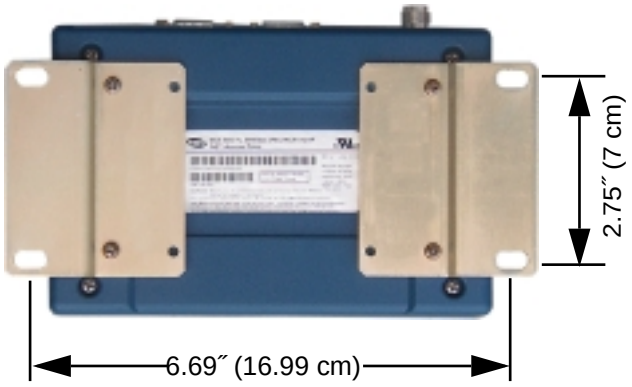


Figure 6-3. Mounting Brackets Spacing—Remote

6.1.2 Site Selection

Suitable installation sites should provide:

- Protection from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna, interface or other required cabling
- Antenna location that provides as unobstructed a transmission path as possible in the direction of the associated station(s)

These requirements can be quickly determined in most cases. A possible exception is the last item—verifying that an unobstructed transmission path exists. Radio signals travel primarily by line-of-sight, and obstructions between the sending and receiving stations will affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below will provide helpful background.

6.1.3 Terrain and Signal Strength

While the license-free 900 MHz band offers many advantages for data transmission services, signal propagation is affected by attenuation from obstructions such as terrain, foliage or buildings in the transmission path.

A line-of-sight transmission path between the central transceiver and its associated transceiver site(s) is highly desirable and provides the most reliable communications link.

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of –100 dBm or stronger will provide acceptable performance in many systems. While the equipment will work at lower-strength signals, signals stronger than

– 90 dBm provide a “fade margin” of 15 dB to account for variations in signal strength that may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port of the transceiver. (See *“Antenna Direction Optimization”* on Page 122 for details.)

6.1.4 Antenna & Feedline Selection

Antennas

The equipment can be used with a number of antennas. The exact style used depends on the physical size and layout of a system. Contact your MDS representative for specific recommendations on antenna types and hardware sources.

In general, an omnidirectional antenna (Figure 6-4) is used at the Access Point station site. This provides equal coverage to all of the Remote sites.

NOTE: Antenna polarization is important. If the wrong polarization is used, a signal reduction of 20 dB or more will result. Most systems using a gain-type omnidirectional antenna at the Access Point station employ vertical polarization of the signal; therefore, the Remote antenna(s) must also be vertically polarized (elements oriented perpendicular to the horizon).

When required, horizontally polarized omnidirectional antennas are also available. Contact your MDS representative for details.

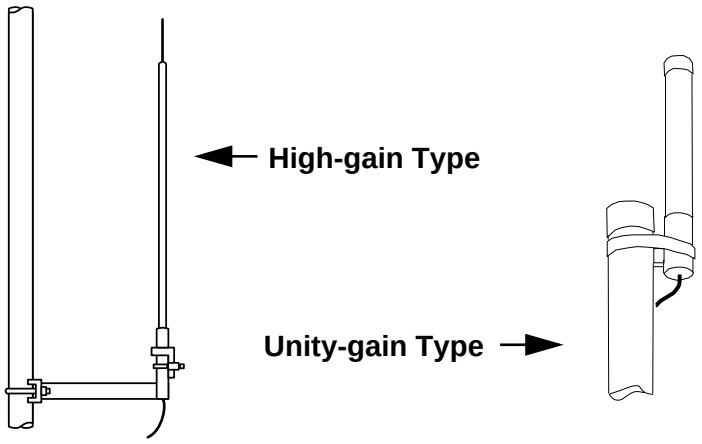


Figure 6-4. Typical Omnidirectional Antennas

At Remote sites and units in point-to-point LANs, a directional Yagi (Figure 6-5) antenna is generally recommended to minimize interference to and from other users. Antennas are available from a number of manufacturers.

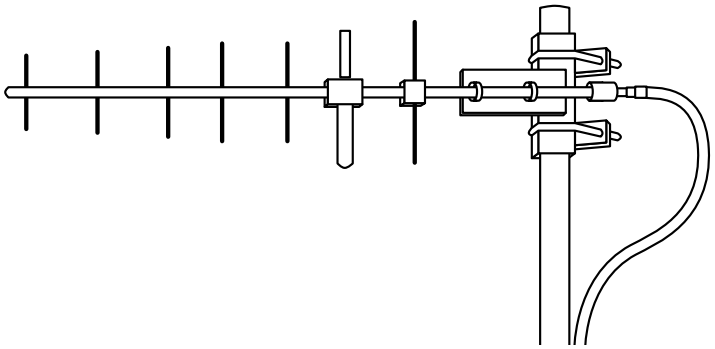


Figure 6-5. Typical Yagi Antenna (mounted to mast)

Feedlines

The choice of feedline used with the antenna should be carefully considered. Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept as short as possible to minimize signal loss.

For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive type such as Type RG-8A/U may be acceptable. Otherwise, we recommend using a low-loss cable type suited for 900 MHz, such as Andrew Corp. Heliax®.

Table 6-1 lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of cable at 900 MHz. The choice of cable will depend on the required length, cost considerations, and the amount of signal loss that can be tolerated.

Table 6-1. Length vs. loss in coaxial cables at 900 MHz

Cable Type	10 Feet (3.05 m)	50 Feet (15.24 m)	100 Feet (30.48 m)	500 Feet (152.4 m)
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable Loss
1/2 inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

Table 6-2 outlines the minimum lengths of RG-214 coaxial cable that must be used with common MDS omnidirectional antennas in order *to maintain compliance with FCC maximum limit of +36 dBm*.

Table 6-2. Minimum Feedline Length versus Antenna Gain

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	Power Level @ Minimum Length
Unity (0 dB)	2.15 dBi	3 meters (1.0 dB)	+31.15 dBi
3 dBd	5.15 dBi	3 meters (1.0 dB)	+34.15 dBi
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBi

6.1.5 Conducting a Site Survey

If you are in doubt about the suitability of the radio sites in your system, it is best to evaluate them before a permanent installation is begun. This can be done with an on-the-air test (preferred method); or indirectly, using path-study software.

An on-the-air test is preferred because it allows you to see firsthand the factors involved at an installation site and to directly observe the quality of system operation. Even if a computer path study was conducted earlier, this test should be done to verify the predicted results.

The test can be performed by first installing a radio and antenna at the proposed Access Point (AP) station site (one-per-system). Then visit the Remote site(s) with a transceiver and a hand-held antenna. (A PC with a network adapter can be connected to each radio in the network to simulate data during this test using the PING command.)

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value. (See *"Antenna Direction Optimization"* on Page 122 for details.) If adequate signal strength cannot be obtained, it may be necessary to mount the station antennas higher, use higher gain antennas, select a different site or consider installing a repeater station. To prepare the equipment for an on-the-air test, follow the general installation procedures given in this guide and become familiar with the operating instructions found in the *CHAPTER-* beginning on Page 113.

6.1.6 A Word About Radio Interference

The transceivers share the radio-frequency spectrum with other 900 MHz services and other Part 15 (unlicensed) devices in the USA. As such, near 100% error-free communications may not be achieved in a given location, and some level of interference should be expected. However, the radio's flexible design and hopping techniques should allow adequate performance as long as care is taken in choosing station location, configuration of radio parameters and software/protocol techniques.

In general, keep the following points in mind when setting up your communications network.

1. Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.

2. Use a directional antenna at Remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, that minimizes interference to (and from) stations located outside the pattern.

3. If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization.

   Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.

4. Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each Network Address has a different hop pattern. Additional isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical.

5. If constant interference is present in a particular frequency zone, it may be necessary to "skip" that zone from the radio's hopping pattern. The radio includes built-in software to help users identify and remove blocked frequency zones from its hopping pattern. (See *"Skip Zone Options Menu"* on Page 41 for more information.)

6. If interference problems persist even after skipping some zones, try reducing the length of data streams. Groups of short data streams have a better chance of getting through in the presence of interference than do long streams.

7. The power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your MDS sales or Technical Support Department for more information.

6.1.7 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm (1 Watt) RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable RF output may be limited to less than 1 watt (For example, 100 mW /+20 dBm). Be sure to check for and comply with the requirements for your area.

Calculating System Gain

To determine the maximum allowable power setting of the radio, perform the following steps:

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)

2. Subtract the antenna system gain from 36 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.

3. If the maximum transmitter power allowed is less than 30 dBm, set the power to the desired level using the entraNET Management System.
   (**Main Menu>Radio Configuration>RF Output Power Setpoint**)

For convenience, Table 6-3 lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 6 dB or less entitles you to operate the radio at full power output –30 dBm (1 Watt).

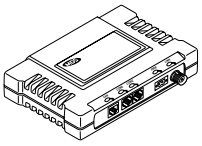
Table 6-3. Antenna System Gain vs. Power Output Setting (USA)

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (in dBm)	EIRP (in dBm)
6 (or less)	30	36
8	28	36
10	26	36
12	24	36
14	22	36
16	20	36

* Most antenna manufacturers rate antenna gain in dBd in their literature. To convert to dBi, add 2.15 dB.

† Feedline loss varies by cable type and length. To determine the loss for common lengths of feedline, see Table 6-1 on Page 108.

To convert dBm to Watts, refer to *dBm-WATTS-VOLTS CONVERSION CHART*, on Page 113.



6.2 dBm-WATTS-VOLTS CONVERSION CHART

Table 6-4 is provided as a convenience for determining the equivalent voltage or wattage of an RF power expressed in dBm.

Table 6-4. dBm-Watts-Volts Conversion—for 50 ohm systems

dBm	V	Po
+53	100.0	200W
+50	70.7	100W
+49	64.0	80W
+48	58.0	64W
+47	50.0	50W
+46	44.5	40W
+45	40.0	32W
+44	32.5	25W
+43	32.0	20W
+42	28.0	16W
+41	26.2	12.5W
+40	22.5	10W
+39	20.0	8W
+38	18.0	6.4W
+37	16.0	5W
+36	14.1	4W
+35	12.5	3.2W
+34	11.5	2.5W
+33	10.0	2W
+32	9.0	1.6W
+31	8.0	1.25W
+30	7.10	1.0W
+29	6.40	800mW
+28	5.80	640mW
+27	5.00	500mW
+26	4.45	400mW
+25	4.00	320mW
+24	3.55	250mW
+23	3.20	200mW
+22	2.80	160mW
+21	2.52	125mW
+20	2.25	100mW
+19	2.00	80mW
+18	1.80	64mW
+17	1.60	50mW
+16	1.41	40mW
+15	1.25	32mW
+14	1.15	25mW
+13	1.00	20mW
+12	.90	16mW
+11	.80	12.5mW
+10	.71	10mW
+9	.64	8mW
+8	.58	6.4mW
+7	.500	5mW
+6	.445	4mW
+5	.400	3.2mW
+4	.355	2.5mW
+3	.320	2.0mW
+2	.280	1.6mW
+1	.252	1.25mW

dBm	V	Po
0	.225	1.0mW
-1	.200	.80mW
-2	.180	.64mW
-3	.160	.50mW
-4	.141	.40mW
-5	.125	.32mW
-6	.115	.25mW
-7	.100	.20mW
-8	.090	.16mW
-9	.080	.125mW
-10	.071	.10mW
-11	.064	
-12	.058	
-13	.050	
-14	.045	
-15	.040	
-16	.0355	

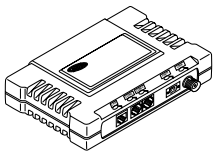
dBm	mV	Po
-17	31.5	
-18	28.5	
-19	25.1	
-20	22.5	.01mW
-21	20.0	
-22	17.9	
-23	15.9	
-24	14.1	
-25	12.8	
-26	11.5	
-27	10.0	
-28	8.9	
-29	8.0	
-30	7.1	.001mW
-31	6.25	
-32	5.8	
-33	5.0	
-34	4.5	
-35	4.0	
-36	3.5	
-37	3.2	
-38	2.85	
-39	2.5	
-40	2.25	.1µW
-41	2.0	
-42	1.8	
-43	1.6	
-44	1.4	
-45	1.25	
-46	1.18	
-47	1.00	
-48	0.90	

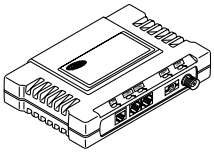
dBm	mV	Po
-49	0.80	
-50	0.71	.01µW
-51	0.64	
-52	0.57	
-53	0.50	
-54	0.45	
-55	0.40	
-56	0.351	
-57	0.32	
-58	0.286	
-59	0.251	
-60	0.225	.001µW
-61	0.200	
-62	0.180	
-63	0.160	
-64	0.141	

dBm	µV	Po
-65	128	
-66	115	
-67	100	
-68	90	
-69	80	
-70	71	.1nW
-71	65	
-72	58	
-73	50	
-74	45	
-75	40	
-76	35	
-77	32	
-78	29	
-79	25	
-80	22.5	.01nW
-81	20.0	
-82	18.0	
-83	16.0	
-84	11.1	
-85	12.9	
-86	11.5	
-87	10.0	
-88	9.0	
-89	8.0	
-90	7.1	.001nW
-91	6.1	
-92	5.75	
-93	5.0	
-94	4.5	
-95	4.0	
-96	3.51	
-97	3.2	

dBm	µV	Po
-98	2.9	
-99	2.51	
-100	2.25	.1pW
-101	2.0	
-102	1.8	
-103	1.6	
-104	1.41	
-105	1.27	
-106	1.18	

dBm	nV	Po
-107	1000	
-108	900	
-109	800	
-110	710	.01pW
-111	640	
-112	580	
-113	500	
-114	450	
-115	400	
-116	355	
-117	325	
-118	285	
-119	251	
-120	225	.001pW
-121	200	
-122	180	
-123	160	
-124	141	
-125	128	
-126	117	
-127	100	
-128	90	
-129	80	.1*f*W
-130	71	
-131	61	
-132	58	
-133	50	
-134	45	
-135	40	
-136	35	
-137	33	
-138	29	
-139	25	
-140	23	.01*f*W

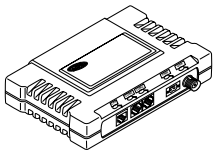




7 TROUBLESHOOTING & RADIO TESTS

7.1 TROUBLESHOOTING 117

7.1.1 Interpreting the Front Panel LEDs 117
7.1.2 Troubleshooting Using the Embedded Management Sys. 118
Ethernet Packet Statistics Menu 120
Serial Port/Remote Serial Statistics Menu 121
Diagnostic Tools 121
7.1.3 Using Logged Operation Events 121
7.1.4 Antenna Direction Optimization 122
Introduction 122
Procedure 122



7.1 TROUBLESHOOTING

Successful troubleshooting of a wireless system is not difficult, but requires a logical approach. It is best to begin troubleshooting at the Access Point unit, as the rest of the system depends on the Access Point for synchronization data. If the Access Point has problems, the operation of the entire wireless network will be affected.

When communication problems are found, it is good practice to begin by checking the simple things. Applying basic troubleshooting techniques in a logical progression can identify many problems.

Multiple Communication Layers

It is important to remember the operation of the network is built upon a radio communications link. On top of that are two data levels— wireless MAC, and the data layer. It is essential that the wireless aspect of the Access Point and the Remotes units to be connected are operating properly before data-layer traffic will function.

Unit Configuration

There are over 50 user-configurable parameters in the entraNET Management System. Do not overlook the possibility that human-error may be the cause of the problem. With so many possible things to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help you avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files,

See *"Using Configuration Scripts"* on Page 71.

Factory Assistance

If problems cannot be resolved using the guidance provided here, review the MDS Web site's technical support area for recent software/firmware updates, general troubleshooting help, and service information. Additional help is available through the MDS Technical Support Department. (See "TECHNICAL ASSISTANCE" on the inside of the rear cover.)

7.1.1 Interpreting the Front Panel LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of case. They should be the first thing to check whenever a problem is suspected. Table 2-2 on Page 21 describes the function of each status LED. Table 7-1 below provides suggestions for

resolving common system difficulties using the LEDs, and Table 7-3 other simple techniques.

Table 7-1. Troubleshooting Using LEDs—Symptom-Based

Symptom	Problem/Recommended System Checks
PWR LED does not turn on.	a. Voltage too low or wrong polarity—Check for the proper supply voltage at the power connector (6–30 Vdc). See Figure 2-5 on Page 16 for polarity details. b. Transient condition—Cycle the power and wait (≈ 30 seconds) for the unit to reboot. Recheck for normal operation.
LINK LED does not turn on.	a. Network Address of Remote not identical to desired Access Point—Verify that the system has a unique Network Address. b. Not yet associated with an Access Point with the same Network Address. Check the "Status" of the unit's process of associating with the Access Point. Use the **RADIO** command. c. Poor Antenna System—Check the antenna, feedline and connectors. Reflected power should be less than 10% of the forward power reading (SWR 2:1 or lower).
PWR LED is blinking.	a. Blinking indicates an alarm condition exists. b. View Current Alarms and Event Log and correct the problem if possible. (See *"Using Logged Operation Events"* on Page 121) c. Blinking will continue until the source of the alarm is corrected, for example, a valid IP address is entered, etc.
LAN LED does not turn on.	a. Verify the Ethernet cable is connected at both ends. b. Verify that the proper type of Ethernet cable is used: straight-through, or crossover. See Table 7-2 below for proper cable type.
COM1 or COM2 LED does not show traffic.	a. Check configuration of COM port and Remote Serial Gateway settings.

Table 7-2 shows the proper type of Ethernet cable to use with the radio when connecting to external devices.

Table 7-2. Proper Ethernet Cable Type

Radio Type	Connected Device	Cable Type
Access Point	LAN	Straight Through
Access Point	PC	Crossover
Remote	PC	Straight Through
Remote	LAN	Not Permitted

7.1.2 Troubleshooting Using the Embedded Management System

If you have looked over and tried the things mentioned in Table 7-1and still have not resolved the problem, there are some additional tools and techniques that can be used. The embedded Management System is a

good source of information that may be used remotely to provide preliminary diagnostic information, or may even provide a path to correcting the problem.

Table 7-3. Basic Troubleshooting with the entraNET MS

Symptom	Problem/Recommended System Checks
Remote does not connect	a. Verify the AP has sufficiently large number in the “Max Remotes” parameter of the Network Configuration Menu. b. If “Approved Remotes” is enabled on the Security Configuration menu (at the AP), verify the correct serial number is listed in the Approved Remotes List. c. On the Remote, if “Restrict” is turned on in the APLIST command, verify the Access Point is included in the list of Approved APs.
Cannot access the entraNET AP Menu (through COM1)	a. If the unit is an AP, connect via Telnet or Web browser b. Disable the serial mode for COM1 (Serial Gateway Configuration>Com1 Serial Data Port>Status>Disabled) Or, if you know the unit’s data configuration: a. Connect to COM 1 via a terminal set to VT100 and the port’s data baud rate. b. Type “+++ [ENTER]” c. Change the terminal’s baud rate to match the transceiver’s Console Baud Rate. d. Type “+++ [ENTER]”
Cannot access the Remote’s command interface	a. Connect to the AP’s menu and manage the Remote via the Serial Configuration menu. Check the configuration for COM1 or 2, as applicable.
Display on terminal/Telnet screen garbled	a. Verify the terminal/terminal emulator or Telnet application is set to VT100. Restart terminal program.
Cannot pass IP data to WAN.	a. Verify the AP’s IP settings. b. Use the PING command to test communication with the AP and endpoints connected to Remote radios in the local radio system. c. If successful with local PING, attempt to PING an IP unit attached to a radio. d. If successful with the LAN PINGs, try connecting to a known unit in the WAN.
Wireless Retries too high.	Possible Radio Frequency Interference— a. If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations. b. Try skipping some zones where persistent interference is suspected or packets-per-zone are disparate. c. The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance.
Password forgotten.	a. Connect to the transceiver using a terminal through the COM1 Port. b. Call MDS. Get a password-resetting Authorization Key. c. Enter the Authorization Key at the login prompt as a password.

The following is a summary of how several screens in the entraNET Management System can be used as diagnostic tools. For information on how to connect to the entraNET Management System See *"STEP 3—CONFIGURE THE TRANSCEIVERS"* on Page 17.

Ethernet Packet Statistics Menu

(See Figure 3-32 on Page 60 for detailed information)

This screen provides detailed information on data exchanges between the unit being viewed and the network through the network layer. These include:

Wireless Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Packets dropped
- Receive errors
- Retries
- Retry errors

Ethernet Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Packets dropped
- Receive errors
- Retries
- Retry errors
- Lost carrier detected

The most significant fields are *Retries*, *Retry Errors*, *Receive Errors*, and *Lost Carrier Detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost Carrier Detected* value is greater than a few dozen, there may be trouble with radio-frequency interference or a radio link of marginal strength. See *"Antenna Direction Optimization"* on Page 122 for tips on maximizing the quality of the received signal.

When troubleshooting throughput quality issues, a check should also be made of the *Radio Packet Statistics* screen shown in Figure 3-33 on Page 61. This menu provides a review of packet statistics from a radio link (RF) perspective.

It is also helpful to check the RSSI of incoming signals. If the RSSI levels in each zone are within a few decibels (dB) of each other, but less than –90 dBm, then a check should be made of the aiming of the antenna system. See *"Antenna Direction Optimization"* on Page 122 for details.

NOTE: The average signal level should be –95 dBm or stronger for reliable performance with an allowance for fade margin.

Another place to look for trouble is in the Packets Received by Zone. The packets should be evenly distributed across all zones (1-5% variation). If they are not, interference in the disparate zones should be sus-

pected. Blocking these zones may eliminate or reduce harmful interference. (See *"Skip Zone Options Menu"* on Page 41 for more information.)

When dealing with radio interference troubles, be sure to review Section 6.1.6, beginning on Page 109.

Serial Port/Remote Serial Statistics Menu

(See Figure 3-31 on Page 59 for detailed information)

This screen provides top-level information on data exchanges between the unit's serial ports and the network through the wireless and the Ethernet (data) layers. These include:

- Bytes In On Port *xxx*
- Bytes In On Socket *xxx*
- Bytes Out On Port *xxx*
- Bytes Out On Socket *xxx*

You can use this information as an indicator of port activity at the data and IP levels.

Diagnostic Tools

(See MAINTENANCE/TOOLS, on Page 65)

The AP's Maintenance menu contains a tool that is especially useful to network technicians—the Ping Utility. The Ping Utility can be used to verify reachability of Ethernet devices connected to the network.

7.1.3 Using Logged Operation Events

(See Event Log Menu, on Page 61)

The transceiver's microprocessor monitors many operational parameters and logs them as various classes of "events". If the event is one that affects performance, it is an "alarmed". There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes and external access to the entraNET Management System. Informational events are stored in temporary (RAM) memory that will be lost in the absence of primary power, and Alarms will be stored in permanent memory (Flash memory) until cleared by user request. Table 3-1 summarizes these classifications.

Table 7-4. Event Classifications

Level	Description/Impact	Storage
Informational	Normal operating activities	Flash Memory
Minor	Does not affect unit operation	RAM
Major	Degraded unit performance but still capable of operation	RAM
Critical	Prevents the unit from operating	RAM

These various events are stored in the transceiver's "Event Log" and can be a valuable aid in troubleshooting unit problems or detecting attempts at breaching network security.

7.1.4 Antenna Direction Optimization

Introduction

The wireless network integrity depends, in a large part, on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than –90 dBm will provide the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage and man-made obstructions become more influential and the use of directional antennas at Remote locations becomes necessary. Directional antennas usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to tell you when the antenna is in a position that provides the optimum received signal.

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements will be displayed by the entraNET Management System.

The measurement and antenna alignment process will usually take 10 or more minutes at each transceiver.

The path to the Management System menu item is shown in bold text below each step of the procedure.

Procedure

1. Verify the Remote is associated with an Access Point unit. Observe the condition of the LINK LED.
   LINK LED = On or Blinking

   This will indicate that you have an adequate signal level for the measurements and it is safe to proceed.

2. View and record the *Radio Retries and No Ack* counts on the Radio Packet Statistics screen (Figure 3-33 on Page 61). This information will be used later.

3. Clear the *Radio Statistics* history.

4. Read the RSSI level at the Remote.
   (RADIO RSSI=)

5. Optimize the RSSI by slowly adjusting the direction of the antenna and watching for a peak in received signal strength. Get the RSSI indication several times after making each adjustment so that the

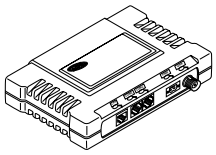
RSSI accurately reflects any change in the link signal strength. The higher the indication (less negative) the stronger the signal level (i.e., –60 is better than –70).

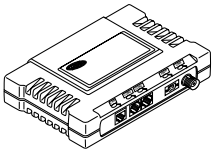
6. View the *Radio Retries* and *No Ack* counts at the point of maximum RSSI level. They should be the same or lower than the previous reading.

   (Main Menu>Performance Information>Packet Statistics>Wireless Packet Statistics)

   If the RSSI peak results in an increase in the *Radio Retries* and *No Ack* counts, the antenna may be aimed at an undesired signal source. Try a different antenna orientation.

End of procedure





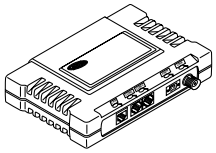
8 TECHNICAL REFERENCE

Contents

8.1 DATA INTERFACE CONNECTORS 127

8.1.1 Ethernet/LAN Port (AP, Ethernet Remote) 127
8.1.2 COM1 Port (AP, Remotes) 128
8.1.3 COM2 Port (AP, Serial Remotes) 128

8.2 TECHNICAL SPECIFICATIONS 129



8.1 DATA INTERFACE CONNECTORS

Three types of data interface connectors are used on entraNET transceivers. The first, the LAN Port, is a metallized RJ-45 connector. The other two are standard modular types—RJ 12 for the COM1 port, and RJ-45 for the COM2 port. This section provides illustrations and pinout information for all of these data connectors.

CAUTION

RADIO INTERFERENCE POTENTIAL

The transceiver meets U.S.A.'s FCC Part 15, Class A limits when used with shielded data cables not exceeding 3 feet/0.9 meters in length.

8.1.1 Ethernet/LAN Port (AP, Ethernet Remote)

This port is used to connect to an Ethernet network at an AP or to the endpoint of a Remote.

- To connect a PC directly to the AP's Ethernet port, an RJ-45 to RJ-45 cross over cable is required. At the Remote, a straight through cable is required.
- To connect the AP to a Ethernet hub or bridge, use a straight-through cable.

The connector uses standard Ethernet RJ-45 cables and wiring. The pinout information below may be used to construct a custom cable, if required.

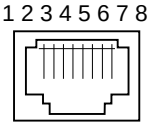


Figure 8-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

Pin	Functions	Ref.
1	Transmit Data (TX)	High
2	Transmit Data (TX)	Low
3	Receive Data (RX)	High
4	Unused	
5	Unused	
6	Receive Data (RX)	Low
7	Unused	
8	Unused	

8.1.2 COM1 Port (AP, Remotes)

A PC may be connected to the Remote transceiver's COM1 port (RJ-12) for diagnostics and configuration. Pinout information for the COM1 port is provided in Figure 8-2 and Table 8-1.

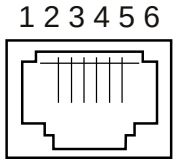


Figure 8-2. COM1 Port (DCE)
Viewed from the outside of the radio

Table 8-1. COM1 Port Pinout, RS-232 Interface

Pin	Functions	COM1 Port (DCE)
1	Unused	
2	Unused	
3	Unused	
4	Transmit Data (TXD)	In
5	Receive Data (RXD)	Out
6	Ground	—

8.1.3 COM2 Port (AP, Serial Remotes)

A terminal device (DTE) may be connected to the transceiver's COM2 port (RJ-45) for payload data connection. Pinout information for the COM2 port is provided in Figure 8-3 and Table 8-2.

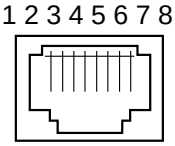


Figure 8-3. COM2 Port (DCE)
Viewed from the outside of the radio

Table 8-2. COM2 Port, EIA-232 Interface

Pin	Functions	COM2 Port (DCE)
1	Unused	
2	Data Carrier Detect (DCD)	Out
3	Data Terminal Ready (DTR)	In
4	Signal Ground (GND)	—

Table 8-2. COM2 Port, EIA-232 Interface *(Continued)*

Pin	Functions	COM2 Port (DCE)
5	Receive Data (RXD)	Out
6	Transmit Data (TXD)	In
7	Clear-to-Send (CTS)	Out
8	Request-to-Send (RTS)	In

8.2 TECHNICAL SPECIFICATIONS

GENERAL

Temperature Range:	–40° C to +70° C (–40° F to 158° F)
Humidity:	95% at +40° C (104° F); non-condensing
Primary Power:	6–30 Vdc (13.8 Vdc Nominal)
Supply Current (typical):	11 Watts Maximum @ 1 Watt RF Output
Transmit:	AP: 800 mA @ 13.8 Vdc Remote: 600 mA
Receive:	AP: 300 mA @ 13.8 Vdc Remote:150
Sleep (Remote):	<20 mA @ 12 Vdc
Shutdown:	<1 mA @ 12 Vdc
MTBF:	35 Years (Telcordia Method 1, Case 3)
Size (Excluding mtg. hardware):	1.5" x 6" x 4" (H x W x D) 3.8 x 15.2 x 10.2 cm
Weight:	0.9 kg / 2 lb (AP) 0.43 kg/0.95 lb (Remote)
Case:	Cast Aluminum
Boot Time:	AP: ≈ 30 seconds
	Remote: ≈ 1 seconds
Time Required to Connect with Access Point:	<1 second typical

APPROVALS/HOMOLOGATION

- FCC Part 15.247
- Industry Canada RSS-210 and RSS-139
- UL/CSA Class 1, Div. 2; Groups A, B, C and D hazardous locations
- Contact MDS for information on availability and governmental approvals in other countries

EMBEDDED MANAGEMENT SYSTEM

Access Point:

- HTTP (Embedded Web server)
- Text-based menu on COM1 serial port
- Telnet

Remote Radios:	• Command line via COM1 port

DATA CHARACTERISTICS

PORTS (AP):

Ethernet:

Interface Connectors:	RJ-45 Standard, 10-Base-T
Data Rate:	10 Mbps

COM1, COM2:

Signaling Standard:	EIA-232/V.24
Interface Connectors:	COM1: RJ-12, COM2: RJ-45, EIA-561
Interface:	COM1: Non-Handshaking / COM2: DCE
Data Rate:	1200–115,200 bps asynchronous

PORTS (Remote):

Ethernet:

Interface Connectors:	RJ-45 Standard, 10-Base-T
Data Rate:	10 Mbps

COM1, COM2:

Signaling Standard:	EIA-232/V.24
Interface Connectors:	COM1: RJ12, COM2 RJ-45, EIA-561
Interface:	COM1: Non-handshaking / COM2: DCE
Data Rate:	1200–115,200 bps asynchronous

PROTOCOLS:

- IEEE 802.3 (Ethernet)
- IP/Ethernet (ICMP, UDP, TCP, ARP)
- Clear-channel mode for serial async multidrop protocols including: Modbus, DNP.3, Bisync, BSAP, DF1, TotalFlow, Poll Select

RADIO CHARACTERISTICS

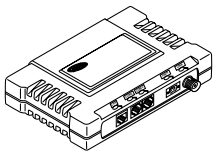
GENERAL:

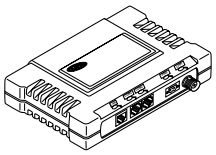
Frequency Range:	902–928 MHz ISM Band
Frequency Hopping Range:	Eight user-configurable 3.2 MHz-wide zones, each containing 16 frequencies
Hop Pattern:	Based on Network Address
Frequency Stability:	30 ppm

TRANSMITTER:

Power Output (at antenna connector):	0.1 to 1.0 watt (+20 dBm to +30 dBm) ±3.0 dB, *set by user*
Duty Cycle:	Continuous
Modulation Type:	Binary CPFSK
Output Impedance:	50 Ohms
Spurious:	–67 dBc

Occupied Bandwidth:	200 kHz
RECEIVER:	
Type:	Double conversion superheterodyne
Sensitivity:	–105 dBm @ 106 kbps < $1x10^{-6}$ BER
Intermodulation:	59 dB Minimum (EIA)
Desensitization:	70 dB
Spurious:	60 dB





9 DEFINITIONS OF TERMS

If you are new to wireless IP/Ethernet systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of the transceiver system.

Access Point (AP)—The transceiver in the network that provides synchronization information to one or more connected Remote units.

Antenna System Gain—A figure, normally expressed in dB, representing the power increase resulting from the use of a gain-type antenna. System losses (from the feedline and coaxial connectors, for example) are subtracted from this figure to calculate the total antenna system gain.

AP—See *Access Point*

Associated—Condition in which the frequency hopping pattern of the Remote is synchronized with the Access Point station in a network, is recognized by the AP, and is ready to pass traffic.

Authorization Key—Alphanumeric string (code) that is used to enable additional capabilities in a transceiver.

Bit—The smallest unit of digital data, often represented by a one or a zero. Eight bits (plus start, stop, and parity bits) usually comprise a byte.

Bits-per-second—See *BPS*.

BPS—Bits-per-second (bps). A measure of the information transfer rate of digital data across a communication channel.

Byte—A string of digital data usually made up of eight data bits and start, stop and parity bits.

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

Data Terminal Equipment—See *DTE*.

dBi—Decibels referenced to an “ideal” isotropic radiator in free space. Frequently used to express antenna gain.

dBm—Decibels referenced to one milliwatt. An absolute unit used to measure signal power, as in transmitter power output, or received signal strength.

DCE—Data Circuit-terminating Equipment (or Data Communications Equipment). In data communications terminology, this is the "modem" side of a computer-to-modem connection. COM1 and COM2 Port of the transceivers are set as DCE.

Decibel (dB)—A measure of the ratio between two signal levels. Frequently used to express the gain (or loss) of a system.

Device Mode—The operating mode/role of a transceiver (Access Point or Remote) in a wireless network.

DHCP (Dynamic Host Configuration Protocol)—An Internet standard that allows a client (i.e. any computer or network device) to obtain an IP address from a server on the network. This allows network administrators to avoid the tedious process of manually configuring and managing IP addresses for a large number of users and devices.

When a network device powers on, if it is configured to use DHCP, it will contact a DHCP server on the network and request an IP address. The DHCP server will provide an address from a pool of addresses allocated by the network administrator. The network device may use this address on a "time lease" basis or indefinitely depending on the policy set by the network administrator.

Digital Signal Processing—See *DSP*.

DSP—Digital Signal Processing. DSP circuitry is responsible for the most critical real-time tasks; primarily modulation, demodulation, and servicing of the data port.

DTE—Data Terminal Equipment. A device that provides data in the form of digital signals at its output. Connects to the DCE device.

Encapsulation—Process in by which, a complete data packet, such as Modbus frame or any other polled asynchronous protocol frame, is placed in the data portion of another protocol frame (for example, IP) to be transported over a network. Typically this action is done at the receiving end, before being sent as an IP packet to a network. A similar reversed process is applied at the other end of the network extracting the data from the IP envelope, resulting in the original packet in the original protocol.

Endpoint—Data equipment connected to the ports of the radio.

Fade Margin—The greatest tolerable reduction in average received signal strength that will be anticipated under most conditions. Provides an allowance for reduced signal strength due to multipath, slight antenna

movement or changing atmospheric losses. A fade margin of 15 to 20 dB is usually sufficient in most systems.

Frame—A segment of data that adheres to a specific data protocol and contains definite start and end points. It provides a method of synchronizing transmissions.

Frequency Hopping—The spread spectrum technique used by the transceivers, where two or more associated radios change their operating frequencies several times per second using a set pattern. Since the pattern appears to jump around, it is said to "hop" from one frequency to another.

Frequency Zone—The transceiver uses up to 80 discrete channels in the 902 to 928 MHz spectrum. A group of 16 channels is referred to as a zone; in total there are 8 zones.

Hardware Flow Control—An transceiver feature used to prevent data buffer overruns when handling high-speed data from the connected data communications device. When the buffer approaches overflow, the radio drops the clear-to-send (CTS) line, that instructs the connected device to delay further transmission until CTS again returns to the high state.

Host Computer—The computer installed at the master station site, that controls the collection of data from one or more remote sites.

HTTP—Hypertext Transfer Protocol

IAPP (inter-Access Point Protocol)—A protocol by which access points share information about the stations that are connected to them. When a station connects to an access point, the access point updates its database. When a station leaves one access point and roams to another access point, the new access point tells the old access point, using IAPP, that the station has left and is now located on the new access point.

ICMP—Internet Control Message Protocol

IEEE—Institute of Electrical and Electronic Engineers

Image (File)—Data file that contains the operating system and other essential resources for the basic operation of the transceiver's CPU.

LAN—Local Area Network

Latency—The delay (usually expressed in milliseconds) between when data is applied at the transmit port at one radio, until it appears at the receive port at the other radio.

MAS—Multiple Address System. A radio system where a central master station communicates with several Remote stations for the pur-

pose of gathering telemetry data. Figure 1-2 on Page 6 shows an example of an MAS system.

MCU—Microcontroller Unit. This is the processor responsible for controlling system start-up, synthesizer loading, hop timing, and key-up control.

MD5—A highly secure data encoding scheme. MD5 is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint". This fingerprint is "non-reversible", it is computationally infeasible to determine the file based on the fingerprint. For more details check out "RFC 1321" on the Internet.

Microcontroller Unit—See *MCU.*

Mobility—Refers to a station that moves about while maintaining active connections with the network. Mobility generally implies physical motion. The movement of the station is not limited to a specific network and IP subnet. In order for a station to be mobile it must establish and tear down connections with various access points as it moves through the access points' territory. In order to do this, the station employs roaming and Mobile IP.

Mode—*See Device Mode.*

MTBF—Mean-Time Between Failures

Multiple Address System (MAS)—See *Point-Multipoint System.*

Network Address—User-selectable integer that is used to identify a group of transceivers that form a communications network. The Access Point and all Remotes within a given system should have the same network address.

Network-Wide Diagnostics—An advanced method of controlling and interrogating MDS radios in a radio network.

PING—Packet INternet Groper. Diagnostic message generally used to test reachability of a network device, either over a wired or wireless network.

Point-Multipoint System—A radio communications network or system designed with a central control station that exchanges data with a number of Remote locations equipped with terminal equipment.

Poll—A request for data issued from the host computer (or master PLC) to a Remote radio.

Portability—Refers to the ability of a transceiver to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a transceiver located in one place and

connected to an access point can be turned off, moved to another place, turned back on, and when the right information is entered can immediately reconnect to the access point without user intervention.

PLC—Programmable Logic Controller. A dedicated microprocessor configured for a specific application with discrete inputs and outputs. It can serve as a host or as an RTU.

Remote—A transceiver in a network that communicates with an associated Access Point unit.

Remote Terminal Unit—See *RTU*.

RFI—Radio Frequency Interference

Roaming—A station's ability to automatically switch its wireless connection between various Access Points as the need arises. A station may roam from one AP to another because the signal strength or quality of the AP signal has degraded below what another AP can provide. When two APs are co-located for redundancy, roaming allows the stations to switch between the units to provide a robust network.

Roaming may also be employed in conjunction with Portability where the station has been moved beyond the range of the original AP to which it was associated. As the station comes in range of a new station, it will switch its connection to the stronger signal. Roaming refers to a station's logical, not necessarily physical, move between APs within a specific network and IP subnet.

RSSI—Received Signal Strength Indicator

RTU—Remote Terminal Unit. A data collection device installed at a Remote radio site.

SCADA—Supervisory Control And Data Acquisition. An overall term for the functions commonly provided through an MAS radio system.

Seamless Mode—A technique used in MDS devices that accommodates protocols that do not tolerate gaps in the middle of a frame (e.g., MODBUS™ ASCII). In these protocols, gaps are interpreted by the connected device as an “end-of-frame” indication, which may cause errors. Seamless mode resolves this through the use of buffers.

Skip Zone(s)—Groups of operating channels (frequencies) deleted from the radio transmitter and receiver operating range.

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio. A measurement of relative received signal quality. High ratios will likely result in better signal detection and performance.

STP—Spanning Tree Protocol

Standing-Wave Ratio—See *SWR*.

SWR—Standing-Wave Ratio. A parameter related to the ratio between forward transmitter power and the reflected power from the antenna system. As a general guideline, reflected power should not exceed 10% of the forward power (≈ 2:1 SWR).

TCP—Transmission Control Protocol

Throughput—A measure of the quantity of data sent and the speed with which it is transferred in a network.

TFTP—Trivial File Transfer Protocol

UDP—User Datagram Protocol

WINS—Windows Internet Naming Service. Part of Microsoft Windows NT and 2000 servers that manages the association of workstation names and locations with Internet Protocol addresses. It works without the user or an administrator having to be involved in each configuration change. Similar to DNS.

Zone—See *Frequency Zone*.

IN CASE OF DIFFICULTY...

MDS products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for MDS products is available from our Technical Support Department during business hours (8:00 A.M.–5:30 P.M. Eastern Time). When calling, please give the complete model number of the radio, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved over the telephone, without the need for returning the unit to the factory. Please use one of the following means for product assistance:

Phone: 585 241-5510	E-Mail: TechSupport@microwavedata.com
FAX: 585 242-8369	Web: www.microwavedata.com

FACTORY SERVICE

Component level repair of radio equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your radio to its proper operating specifications.

If return of the equipment is necessary, you will be issued a Service Request Order (SRO) number. The SRO number will help expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the SRO number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an SRO number.

A statement should accompany the radio describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to the radio. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

The radio must be properly packed for return to the factory. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

Microwave Data Systems
Product Services Department
(SRO No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Product Services Group at 585-241-5540 (FAX: 585-242-8400), or vie e-mail at ProductServices@microwavedata.com.

industrial/wireless/performance

Microwave Data Systems Inc.
175 Science Parkway
Rochester, NY 14620
General Business: +1 585 242-9600
FAX: +1 585 242-9620
Web: www.microwavedata.com

A product of Microwave Data Systems Inc.